

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

**IMPLEMENTACIÓN DE UN SERVIDOR/FIREWALL  
GNU/LINUX EN UN ENTORNO ESCOLAR**

**TRABAJO PARA OPTAR AL TÍTULO DE  
BACHILLER ACADÉMICO**

**RAINER SCHUTH HURTADO**

**ASESORES: OLGA CECILIA SUÁREZ POSADA  
HERNANDO VILLA GARZÓN**

**COLEGIO ALEMÁN DE MEDELLÍN  
ÁREAS DE INFORMÁTICA Y DE ESPAÑOL**

**ITAGÜÍ**

**2008**

“La seguridad no es un producto que pueda comprarse en una tienda, pues consiste en un conjunto de políticas, personas, procesos y tecnologías”.

-- Kevin Mitnick

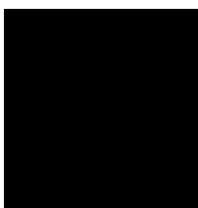
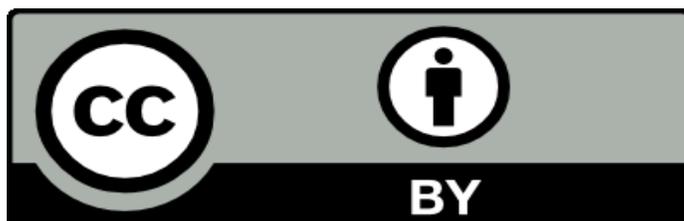
Para la humanidad,  
para todo aquel que busque  
una parte del conocimiento.

## **AGRADECIMIENTOS**

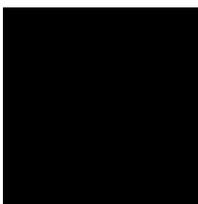
Quiero expresar mis sinceros agradecimientos a Laura, mi novia, quien me apoyó y ayudó mucho y de muchas formas con la elaboración y planificación de este trabajo. Pero sólo estas líneas no son suficientes; parte de este trabajo es tuyo.

Agradezco a todos, y a cada uno, a cada persona, amigo, profesor, a mis padres, a todos, que de una u otra forma me apoyaron y ayudaron a la creación de este proyecto. A todo SB que me dieron la idea para esta trabajo.

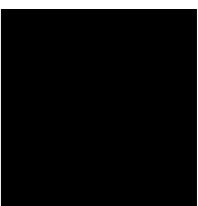
Esta obra está licenciada bajo una *Licencia Atribución 2.5 Colombia* de *Creative Commons*. Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by/2.5/co/> o envíenos una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.



Reconocer al autor.



Copiar, distribuir y comunicar públicamente la obra.



Hacer obras derivadas.

## **Nota del Autor**

Para la fecha en que se finalizó este proyecto (Septiembre de 2008) la versión más actual del *software* a instalar era *ClarkConnect 4.3*. Esta nueva versión tiene mejoras y nuevas herramientas y opciones con respecto a la versión escogida para la realización de este trabajo escrito, pero su compatibilidad y manejo son iguales o similares. En el Apéndice A se encuentra información adicional al respecto.

Además se recomienda que el lector tenga ciertos conocimientos básicos de inglés para entender algunos conceptos que aquí aparecen.

## **Errores en el trabajo**

A pesar de hacer todo lo posible para comprobar los hechos y las cifras, los archivos y la sintaxis, algunos errores inevitablemente se escaparán durante la escritura y el proceso de revisión. Quiero pedir disculpas de antemano por este tipo de errores que existan dentro de estas páginas.

**La mayoría de los componentes de *ClarkConnect* están licenciados bajo *GPL* y otras licencias libres. El logotipo de *ClarkConnect* y el nombre son propiedad de *Point Clark Networks*.**

# ***SOBRE ESTE TRABAJO ESCRITO***

## **I. CONVENCIONES UTILIZADAS**

En este trabajo se usan las siguientes convenciones tipográficas:

- *Cursiva*: se usa para designar marcas comerciales y palabras en otros idiomas. Permite de igual forma identificar nombres de ficheros y conceptos a tener en cuenta.
- *Courier*: empleado para resaltar ejemplos del contenido de archivos o programas, comandos y valores.
- *Courier cursiva*: opciones, código y texto, los cuales deberán ser sustituidos en el código.

## **II. ESTRUCTURA DEL TRABAJO ESCRITO**

Este trabajo está dividido en cuatro partes principales, comenzando por la sección donde se explican las bases y el porqué de este trabajo escrito seguido en segundo lugar por la instalación del sistema operativo. En la tercera parte se ve la configuración e implementación de este y finalmente la administración del sistema.

## **Tabla de contenido**

<b>INTRODUCCIÓN.....</b>	<b>1</b>
<b>CAPÍTULO 1.....</b>	<b>3</b>
1.1 PLANTEAMIENTO DEL PROBLEMA.....	3
1.2 MARCO TEÓRICO.....	5
1.3 PROPÓSITO.....	6
1.4 OBJETIVOS.....	7
1.5 METODOLOGÍA.....	8
1.6 PRESUPUESTO.....	9
1.7 CRONOGRAMA.....	11
1.8 NECESIDAD DE UN FIREWALL, JUSTIFICACIÓN.....	13
<b>CAPÍTULO 2.....</b>	<b>17</b>
2.1 ¿QUÉ ES GNU/LINUX?.....	17
<b>CAPÍTULO 3.....</b>	<b>19</b>
3.1 ¿QUÉ ES UN FIREWALL O CORTAFUEGOS?.....	19
3.2 BENEFICIOS Y LIMITACIONES DE UN FIREWALL.....	20

<b>CAPÍTULO 4.</b> .....	23
4.1 PASOS A SEGUIR PARA LA INSTALACIÓN DEL GNU/LINUX CLARKCONNECT 4.2 COMMUNITY EN UN SERVIDOR.....	23
4.2 PREPARATIVOS.....	25
4.3 REQUERIMIENTOS.....	26
4.3.1 HARDWARE A IMPLEMENTAR.....	29
4.3.2 OPCIÓN 1: .....	30
Tabla 5 - Componentes servidor opción 1.....	30
4.3.3 OPCIÓN 2: .....	31
4.4 COMPATIBILIDAD.....	33
4.5 INSTALACIÓN.....	34
4.5.1 CONFIGURANDO PARA INSTALAR.....	36
4.5.2 “PARTICIONANDO” MANUALMENTE EL DISCO DURO Y CONFIGURACIÓN DEL GESTOR DE ARRANQUE.....	74
 <b>CAPITULO 5</b> .....	 97
5.1 POST-INSTALACIÓN.....	97
5.2 CONFIGURAR LAS INTERFACES DE RED.....	106
5.3.1 INTERFAZ WEB, INGRESO.....	108
5.3.2 CONFIGURACIÓN FINAL DE LA RED.....	117
5.3.3 Proxy SERVER.....	132
5.3.3.1 PASOS PARA CONFIGURAR MS INTERNET EXPLORER®.....	136
5.3.3.2 PASOS PARA CONFIGURAR MOZILLA FIREFOX®.....	138
5.3.4 REGISTRAR EL SERVIDOR.....	146
5.3.5 ACTUALIZAR E INSTALAR SOFTWARE ;	

ADMINISTRACIÓN REMOTA.....	157
5.3.6 CONFIGURACIÓN DEL FIREWALL.....	165
5.3.6.1 OUTGOING (SALIDA).....	165
5.3.6.2 INCOMING (ENTRADA).....	169
5.3.6.4 PORT FORWARDING (REENVÍO DE PUERTOS).....	172
5.3.6.5 PEER-TO-PEER (P2P).....	174
5.3.6.6 ADVANCED -- CREAR REGLAS AVANZADAS.....	175
5.3.6.7 FIREWALL GROUP MANAGER (ADMINISTRADOR DE GRUPOS).....	177
5.3.7 USER ACCOUNT MANAGER (ADMINISTRADOR DE CUENTAS DE USUARIO).....	179
5.3.7.1 USUARIOS.....	179
5.3.7.2 USER PROFILE.....	183
5.3.7.3 GRUPOS.....	183
5.3.7.4 ADMINISTRADOR.....	185
5.3.8 CONTENT FILTER (FILTRADO DE CONTENIDO) .....	189
5.3.8.1 CONFIGURACIÓN DEL CONTROL DE CONTENIDO .....	198
5.3.9 REPORTE.....	201
5.3.9.1 DASHBOARD (TABLERO).....	202
5.3.9.2 CURRENT STATUS (ESTADO ACTUAL DEL SISTEMA).....	203
5.3.9.3 STATISTICS (ESTADÍSTICAS).....	205
5.3.9.3.1 TIPOS DE ESTADÍSTICAS.....	207
5.3.9.4 LOGS (REGISTROS).....	211
5.3.9.5 WEB PROXY REPORT.....	213
5.3.9.6 INTRUSION DETECTION (DETECCIÓN DE INTRUSOS).....	215
5.3.9.10 INTRUSION PREVENTION (PREVENCIÓN DE INTRUSOS).....	221

5.3.10 SYSTEM SETTINGS (SISTEMA).....	224
5.3.10.1 FECHA.....	224
5.3.10.2 LENGUAJE.....	225
5.3.10.3 SERVICIOS (Running Services).....	226
5.3.10.4 SETUP.....	229
5.3.10.5 WEBCONFIG.....	230
5.3.11 SYSTEM TOOLS.....	231
5.3.11.1 ACTUALIZACIONES DEL ANTIVIRUS.....	231
5.3.11.2 COPIA DE SEGURIDAD/RESTAURACIÓN.....	232
5.3.11.3 ENCRYPTED FILE SYSTEM.....	234
5.3.11.4 SHUTDOWN - RESTART.....	236
5.3.12 CONFIGURACIONES ADICIONALES.....	237
5.3.12.1 HOSTS AND DNS SERVERS.....	238
5.3.12.2 NETWORK TOOLS.....	241
5.3.12.3 ACCESS CONTROL (CONTROL DE ACCESO).....	244
<b>CAPÍTULO 6.....</b>	<b>246</b>
6.1 COMANDOS DE ADMINISTRACIÓN DEL SERVIDOR.....	246
6.2 MONITOREO REMOTO DE SERVIDORES.....	247
6.3 COMANDOS DE ADMINISTRACIÓN BÁSICA.....	251
6.4 MONTAR MEDIOS DE ALMACENAMIENTO (mount).....	255
6.5 PERMISOS DE USUARIOS Y DE ARCHIVOS - SEGURIDAD ELEMENTAL.....	256
6.5.1 MANEJO DE PERMISOS CON chmod.....	257
6.5.2 CAMBIO DE PROPIETARIO Y DE GRUPO.....	260
6.6 CONFIGURACIÓN DE RED.....	261

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

6.6.1 ifconfig - EL COMANDO DE LAS INTERFACES.....	262
6.6.2 DNS - /etc/resolv.conf.....	264
6.6.3 dhclient - Dynamic Host Configuration Protocol Client.....	265
6.6.4 ping - EL SONAR DE LA RED.....	265
6.6.5 traceroute - REVISIÓN DEL CAMINO EN LA RED.....	266
<b>APÉNDICES</b> .....	<b>268</b>
A CLARKCONNECT 4.3.....	269
A.1 System Processes.....	269
B GLOSARIO.....	272
C BIBLIOGRAFÍA.....	284



## **INTRODUCCIÓN**

El objetivo de este proyecto y trabajo escrito es desarrollar una solución basada en *software Open Source*<sup>1</sup> y *GNU/Linux*<sup>2</sup>, que a su vez complementada a un *hardware* apropiado, ofrezca prestaciones de seguridad a una red y a sus usuarios como sólo un *Firewall*<sup>3</sup> puede hacerlo.

Para comenzar, en este trabajo escrito deseo que el lector conozca, sepa y se familiarice con los sistemas operativos<sup>4</sup>(SO) *GNU/Linux*, para que su implementación en los diferentes entornos, como en el hogar, el escolar y el laboral, sea menos traumático de lo que se piensa al escuchar y saber poco de un tema desconocido.

Aquí explicare paso a paso cómo y de qué se conforma un Servidor/Firewall y un entorno de red *Windows®/Linux*<sup>5</sup>; cómo el usuario común interactúa con él de forma transparente y cómo un administrador de red controlará mejor su red.

Este documento tomará en cuenta que el usuario que lo lee, aprenderá y

---

1 Código (de *software*) abierto/libre, las licencias no son comerciales y se alienta a distribuirse libremente; puede ser modificado por cualquier persona.

2 *GNU/Linux* es un completo sistema operativo libre y gratuito.

3 Dispositivo que permite o deniega transmisiones en una red.

4 SO: El *software* más importante de un computador, permite una gestión eficaz de sus recursos.

5 Entorno donde los dos SO conviven en una misma red, por lo general el Servidor/Firewall es *GNU/Linux* y las estaciones de trabajo son *Windows®*.

retendrá sus conocimientos, por lo que conforme se avanza a través del documento aumentará gradualmente la dificultad. Adicionalmente, los términos, nombres, códigos y relacionado serán explicados, de ser necesario con ejemplos; si el lector por alguna razón no comprende bien, se recomienda buscar en Internet para resolver la duda, y evitar así posibles confusiones con temas que no se tratarán en este documento. (Enlaces de interés al final del trabajo).

## **CAPÍTULO 1.**

### **1.1 PLANTEAMIENTO DEL PROBLEMA**

Actualmente con el desarrollo continuo de la tecnología, han surgido nuevas formas de comunicarnos en el mundo, quizás todo se debe a la globalización y lo pequeño que es ahora nuestro planeta; día a día estas nuevas tecnologías se imponen sobre las viejas, y con este cambio vienen circunstancias que llevan al mal uso de la información y de la informática.

La problemática viene del uso que se le da a la tecnología, más específicamente: los computadores y la Internet. Los usuarios, en este caso los alumnos y empleados del colegio, tienen la libertad de aprovechar la tecnología en favor del conocimiento, la información y la comunicación, pero a veces esto se hace de formas ilegales o inmorales. Con este trabajo pretendo mostrar, construir y enseñar a montar una muralla, la cual evitará que los usuarios accedan a contenido no permitido ni aceptado por el colegio, como institución educativa.

Lo que deseo mostrar e implementar es una forma de proteger especialmente a los alumnos, aunque no son los únicos, quienes

acceden a contenido no correspondiente con el ámbito académico, ilegal, inapropiado o, indebido para su edad durante las clases, lo cual genera distracción y afecta el ambiente de estudio y de trabajo.

Esta barrera (el *Firewall* o cortafuegos) monitoriza la red observando los contenidos e información que desea ver el usuario y según reglas que el administrador de la red pone en práctica, filtra el contenido dando como resultado el bloqueo de páginas que generan un mal ambiente y sólo permitiendo las educativas o las que aportan conocimiento y saber al alumno. De igual forma, páginas pornográficas y de contenidos ilegales son bloqueadas; esto evita futuros problemas legales que este tipo de contenido puede traer.

Con la nueva implementación del bachillerato internacional, los alumnos tendrán más que nunca acceso a la información (dentro del colegio). El saber calificar y seleccionar esta información no es fácil, y tener una primera barrera que impide desde el principio el acceso a contenido indebido es un gran punto a favor, ayudando a los alumnos a conocer y aprender.

Como punto adicional a favor, se logra una mejor seguridad en la red local del colegio, al igual que se impide que usuarios no autorizados realicen fechorías en la red. Esto beneficia a la institución, porque lo protege contra amenazas informáticas y brinda control sobre los usuarios, y todo esto de una forma muy económica y legal.

Así, mi misión y visión con este trabajo es mostrar y enseñar de una forma muy económica como enfrentar este problema.

## **1.2 MARCO TEÓRICO**

El tema que maneja este trabajo es la seguridad y la protección de la información en un entorno escolar, donde el problema es el de proteger a los usuarios, tanto alumnos como empleados, del contenido al cual acceden, siendo este ilegal o indebido.

Como solución, planteo la implementación de un *Servidor/Firewall GNU/Linux* en el entorno escolar de una forma muy económica para así lograr resolver el problema desde el lado informático.

### **1.3 PROPÓSITO**

El propósito de este trabajo consiste en la implementación de un *Servidor/Firewall GNU/Linux* en un entorno escolar para filtrar el contenido al cual acceden los usuarios.

## **1.4 OBJETIVOS**

- Implementar un servidor *GNU/Linux* de forma muy económica en un entorno escolar.
- Filtrar el contenido al cual los usuarios acceden.
- Brindar seguridad a la red local.
- Impedir la ejecución de código malicioso en la red por usuarios malintencionados de Internet o internos.
- Ayudar al colegio con su labor educativa.
- Aprender y enseñar qué es el *software* libre, más específicamente el sistema operativo *GNU/Linux*.
- Aprender sobre redes informáticas.

## **1.5 METODOLOGÍA**

Seleccionar un computador con el *hardware* necesario para la instalación de un Servidor/*Firewall GNU/Linux*, documentar todo este proceso al igual que la posterior configuración del servidor una vez instalado y su implementación en una red escolar. Para ello se explica paso a paso, de forma detallada, las instrucciones para realizar lo antes mencionado, adicionalmente es complementado con imágenes de los pasos a seguir para una mejor orientación y ayuda al lector.

## **1.6 PRESUPUESTO<sup>6</sup>**

Este tema tiene que ver poco con este trabajo escrito, ya que se pretende minimizar al máximo los gastos de presupuesto sin reducir la calidad del trabajo.

Los gastos del servidor son básicamente los de la instalación, ya que después de su implementación los únicos gastos son: los del administrador de la red y la energía eléctrica que consume el servidor y sus componentes (módem de Internet, encaminador (*router*) y conmutador (*switch*)).

Durante la instalación puede ser necesario la adquisición de 3 metros de cable *UTP categoría 5* con sus respectivos conectores *RJ45*, por el cual pasará la información del servidor a la red. En promedio el metro de cable cuesta \$1,000.00 o \$1,500.00, dando un total (promedio) de \$4,000.00, con el cable ponchado.

Adicionalmente, la compra de una UPS<sup>7</sup>, por aproximadamente \$170,000.00, para el control del flujo de la energía eléctrica, le brindará mas estabilidad y fiabilidad al servidor, al igual que evitará el deterioro causado por las fallas eléctricas.

---

<sup>6</sup> Los precios aquí mostrados son aproximaciones y estos pueden variar al pasar el tiempo. Estos son los precios para septiembre de 2008.

<sup>7</sup> *UPS (Uninterruptible Power Supply)*, o sistema de alimentación ininterrumpida, es un dispositivo, el cual por medio de baterías puede alimentar a otros dispositivos con energía eléctrica por un tiempo limitado.

**Tabla 1 - Tabla de precios**

	<b>Valor total en pesos colombianos (\$)</b>
<i>UPS</i>	\$170,000.00
<i>Cable UTP Cat. 5 ponchado</i>	\$4,000.00
<b>TOTAL</b>	\$174,000.00

## 1.7 CRONOGRAMA

**Tabla 2 - Cronograma de actividades**

Mes 1 (11/08)	-Elección del tema de trabajo: servidor <i>GNU/Linux</i>
Mes 2 (12/08)	-Selección de la distribución de <i>GNU/Linux</i> “ <i>ClarkConnect 4.2</i> ” -Investigación sobre servidores y <i>Firewall</i>
Mes 3 (1/08)	-Continuación de investigación -Adquisición por medio de préstamo de un servidor para laboratorios -Instalación y configuración del <i>Linux</i> en el servidor -Comienzo de pruebas de concepto y análisis de fiabilidad -Realización de imágenes de la instalación
Mes 4 (2/08)	-Comienzo de producción de trabajo escrito -Continuación de pruebas con el servidor -Realización de imágenes de post-instalación y configuración del servidor
Mes 5 (3/08)	-Entrega del primer informe de trabajo -Entrega del anteproyecto (14/03/08) -Continuación de pruebas: comenzar a filtrar

	contenido
Mes 6 (04/08)	-Entrega de proyecto (30/04/08) -Continuación de pruebas: servidor de correo, <i>Firewall</i> , bloqueo de puertos. -Continuación redacción de trabajo
Mes 7 (05/08)	-Finalización del manual de configuración -Continuación del trabajo escrito -Comienza fase final de pruebas
Mes 8 (06/08)	-Continuación del trabajo escrito -Finaliza manual -Comienzo fase de implementación -Finalización del laboratorio
Mes 9 (07/08)	-Revisión del trabajo escrito -Corrección de errores -Completar lo restante al trabajo escrito
Mes 10 (08/08)	-Entrega de borrador final (25/08/08)
Mes 11 (09/08)	-Entrega definitiva del trabajo escrito y práctico (08/09/08) -Sustentación del trabajo escrito

## **1.8 NECESIDAD DE UN FIREWALL, JUSTIFICACIÓN**

El tema central que se tratará es la implementación de un Servidor/*Firewall* (o cortafuegos) en un entorno escolar. Con esta medida se logrará un mayor control del contenido que los alumnos visitan y comparten en Internet como: pornografía, violencia o alusión al consumo de drogas, música y videos con contenido protegido por derechos de autor, archivos infectados con *Malware*<sup>8</sup>, entre otros. Esta protección para el menor de edad es exigida por la constitución en

“el artículo 44, la Ley 679 de 2001, la Ley 765 de 2002, el Código del Menor Decreto 2737 de 1989, Decreto 1524 de 2002, Decreto 1421 de 1993 en su artículo 12, numeral 1°, donde el artículo 44 de la Constitución Nacional dice que los niños 'Serán protegidos contra toda forma de abandono, violencia física o moral, secuestro, venta, abuso sexual, explotación infantil, explotación laboral económica y trabajos riesgosos. Gozarán también de los demás derechos consagrados en la Constitución, en las leyes y en los tratados internacionales ratificados por

---

<sup>8</sup> Es un termino utilizado para el *software* malicioso y se refiere a todo *software* creado para realizar acciones no autorizadas o maliciosas.

Colombia.'

Que la Ley 765 de 2002, 'Por medio de la cual se aprueba el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la pornografía', adoptado en Nueva York, el veinticinco (25) de mayo de dos mil (2.000).

Que el Congreso de la República expidió la Ley 679 de 2001, 'Por medio de la cual se expide el estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.'

Que el Decreto 1355 de 1970 establece las medidas correctivas aplicables en el territorio nacional.

Que el Código del Menor Decreto 2737 de 1989, en su artículo 325, 'Prohibió la venta, préstamo o alquiler a menores de edad de cualquier tipo de material pornográfico. '

Que el Presidente de la República expido el Decreto 1524 de 2002, 'Por el cual reglamenta el artículo 5º de la Ley 679 de 2001', donde se establecen las medidas técnicas y administrativas destinadas a prevenir el acceso a menores de edad en cualquier modalidad de información pornográfica contenida en Internet o en las distintas clases de redes informáticas a las cuales tenga acceso mediante redes

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar globales de información.”<sup>9</sup>

De estas leyes se acuerda que:

“PRIMERO: Todas las Instituciones Educativas Públicas y Privadas, bibliotecas y los establecimientos que mediante computadores tengan acceso a la red de Internet, instalarán los dispositivos tecnológicos para restringir el acceso a material pornográfico nocivo, que afecte el desarrollo integral de los niños, niñas y jóvenes menores de dieciocho (18) años.

SEGUNDO: Las instituciones y establecimientos relacionados en el artículo anterior, contarán a partir de la vigencia del presente acuerdo con un aviso preventivo ubicado en un lugar visible al usuario, en el cual se consignará la restricción de acceso a páginas Web con contenido pornográfico; así mismo, adecuarán en un plazo no mayor a seis meses, *software* o programas que garanticen a los menores de dieciocho (18) años el uso de Internet con

---

9 "Normas sobre el funcionamiento de los establecimientos que prestan el servicio de Internet en Bogotá, D.C" [en línea]. Publicado en [www.dragonjar.us](http://www.dragonjar.us). Febrero 11 de 2008.

restricciones a páginas de pornografía.

TERCERO. Las instituciones y establecimientos relacionados en este acuerdo, designarán como responsable o encargado de la operación de los computadores a una persona mayor de edad."

Para mayor información visitar la siguiente página Web:

<http://www.dragonjar.org/normas-sobre-el-funcionamiento-de-los-establecimientos-que-prestan-el-servicio-de-Internet-en-bogota-dc.xhtml>

## **CAPÍTULO 2.**

### **2.1 ¿QUÉ ES GNU/LINUX?**

Comencemos adentrándonos en el entorno del SO *GNU/Linux*. Pero primero: ¿Qué es *GNU/Linux*? La respuesta para esta pregunta puede ser tanto corta como larga según sea el caso, para éste optemos por una mediana: *GNU/Linux* representa libertad en cuanto a *software*, representa una filosofía, un modo de vida.

*GNU*<sup>10</sup> a finales de los ochenta y principio de los noventa fue un sistema operativo que se estaba creando a partir de una licencia para *software* libre (poder compartir, regalar, modificar, y crear a base de), pero le faltaba el corazón del mismo: el núcleo (*kernel* de ahora en adelante), es lo que facilita a los programas del computador poder acceder al *hardware*, comunicarse con él para poder trabajar en algo tan simple como guardar un documento en el disco duro. En 1991 Linus Torvalds “finalizó” su proyecto, de crear un *kernel* semejante al del SO *UNIX*<sup>11</sup> y lo

---

<sup>10</sup> Acrónimo que significa: *GNU* No es *UNIX* (*GNU* is Not *UNIX*).

<sup>11</sup> SO desarrollado por AT&T en los años 70.

liberó con una licencia libre. Fue en este momento cuando los desarrolladores de *GNU* adoptaron el *kernel* de Linus y lo juntaron con su sistema operativo. Aquí nace *GNU/Linux*. Hoy en día muchas distribuciones (*distros*) y variantes de este SO existen y conviven en la Internet, de donde las podemos descargar, instalar, probar, modificar, etc.

Para este proyecto de implementar un Servidor/*Firewall* en una máquina designada, he escogido una *distro* libre y gratuita que me ayuda a gestionar este proceso. La distribución "*ClarkConnect 4.2 Community*" está enfocada a ser el Servidor/*Firewall* de una red, protegiéndola de accesos no deseados, *Malware* y otras amenazas que hacen que una red pueda sucumbir o los datos de los usuarios se puedan perder o sean amenazados. Además de esto "*ClarkConnect*" puede denegar y permitir lo que los usuarios pueden hacer en una *LAN*<sup>12</sup> y en la Internet; por ejemplo: permitir que los usuarios sólo puedan navegar por páginas legales y permitidas por la institución y denegar el acceso a la red a programas para descargas ilegales (*p2p*<sup>13</sup>) tales como *Ares* y *eMule*; si se desea restringir aun más el uso de la red sólo para propósitos educativos se pueden bloquear programas de mensajería instantánea (en inglés IM, de *Instant messaging*) como *MSN Messenger*, *Yahoo M.* e *ICQ*.

---

12 *Local Area Network (LAN)*, red (de área) local. Un ejemplo es la red con que se conectan los computadores de una institución.

13 *Peer to peer (P2P)*, red donde Servidores se conectan entre sí para compartir archivos.

## **CAPÍTULO 3.**

### **3.1 ¿QUÉ ES UN FIREWALL O CORTAFUEGOS?**

Un *Firewall* funciona como un embudo por el que pasan los datos que circulan por una *LAN*, manteniendo en control a los usuarios restringidos o malintencionados tales como *hackers*, *crackers*<sup>14</sup>, vándalos y espías.

Un *Firewall* también sirve para alertar al Administrador de un posible ataque o fuga de seguridad, por medio de correos electrónicos, mensajes de texto por celular o un mensaje por un *Beeper* las cuales son las maneras más frecuentes de dar alarma.

Todo esto brinda la oportunidad de actuar a tiempo para poder terminar, cerrar o aislar el posible ataque, fuga o problema, y de ser necesario apagar y reiniciar toda la red. Como parte de la gestión de seguridad en la red, después de este tipo de eventos es recomendable realizar un informe y encontrar las causas del suceso para así poder hallar una solución y evitar que pueda suceder de nuevo ante las “narices del administrador”.

---

<sup>14</sup> Persona que por medio de ingeniería inversa realiza: seriales, *keygens*, *cracks*, y viola la seguridad de un sistema informático con beneficio propio.

Adicionalmente, el *Firewall* brinda una mayor seguridad en la red interna de la institución, protegiéndola contra amenazas informáticas y proporcionando control al administrador de la red para supervisar la actividad de los usuarios en ésta y así evitar que ellos, por ejemplo realicen descargas ilegales hacia o desde el Internet. Esta protección brinda seguridad a la institución para evitar problemas legales por infracción a los derechos de autor u otros.

### **3.2 BENEFICIOS Y LIMITACIONES DE UN FIREWALL**

*“Una cadena es tan fuerte como el más débil de sus eslabones.”*

-- proverbio popular

Estos son los puntos a favor para la implementación de un *Firewall* en una red que no posee protección:

Uno beneficio clave de un *Firewall* es la simplificación del trabajo para el Administrador de la red, ya que permite gestionar un solo equipo, el *Firewall*, y así proteger al resto sin modificar los cientos de posibles computadores que existen en la red, evitando que se reduzca su tiempo.

Así se pueden examinar a fondo los archivos de *log*<sup>15</sup> y conocer las páginas a las que se han ingresado, qué procesos o programas han entrado a Internet, y saber qué usuario ha hecho qué. Es muy útil porque para aplicar sanciones se tienen pruebas sólidas de lo sucedido. Cabe aclarar que si uno de los usuarios está empeñado en acceder a la red privada de la institución o quiere filtrar información este lo puede lograr si se empeña en hacerlo. La misión de un *Firewall* es hacer más dura esta labor, más no imposible, porque no se puede; la seguridad total no existe. Por más segura que pueda ser una red siempre habrá un eslabón débil en esta cadena: el factor humano. A una persona se le puede engañar para que revele contraseñas, ayude a descubrir agujeros de seguridad o reemplace al atacante. Esto puede ocurrir de diversas formas, pero un *Firewall* ayuda a prevenir la mayoría de estas: filtrando el *SPAM*<sup>16</sup>, denegando el acceso a la red a programas no permitidos y vigilando lo que el usuario lee en la Web. Un *Firewall* no puede hacer todo esto por sí solo, para ello necesita la ayuda de otro de los componentes que conforman la red: la estación de trabajo que comúnmente se usa con *Windows*®.

Es común encontrarse con estaciones que no están correctamente configuradas y que pueden permitir la fuga de información, la ejecución de un programa no permitido, o una infección de *Malware*.

Para ello se sugiere aplicar estos consejos publicados en el *blog* [www.dragonjar.us](http://www.dragonjar.us) por *4v4t4r*: mirar anexo.

En “Beneficios de un Firewall en Internet” mencionan que “un Firewall de

---

15 Archivos donde se almacena información de un periodo de tiempo sobre cuándo y dónde sucede un evento y quién lo ejecuta.

16 Mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva por correo electrónico.

Internet es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda”<sup>17</sup>.

---

<sup>17</sup> "Beneficios de un Firewall en Internet"[en línea]. Autor: Víctor Ferrusola.

## **CAPÍTULO 4.**

### **4.1 PASOS A SEGUIR PARA LA INSTALACIÓN DEL GNU/LINUX CLARKCONNECT 4.2 COMMUNITY EN UN SERVIDOR**

Para instalar exitosamente se recomienda seguir estos pasos en el orden en que se encuentran. Si se desea cambiar algunas opciones, las cuales no están descritas en los pasos a seguir o no se necesitan emplear para el Servidor/Firewall en el entorno escolar, el usuario tiene completa libertad para hacerlo.

El sistema operativo *GNU/Linux ClarkConnect 4.2* no tiene ninguna garantía según fragmento de los “*Términos de Uso*” del *ClarkConnect* en [http://www.ClarkConnect.com/about/tos\\_pcn.php](http://www.ClarkConnect.com/about/tos_pcn.php) :

**“No Warranties.** Provider does not guarantee that Service will be provided without interruption. Provider does not guarantee quality or timeliness of Service, and will not be held liable for any losses in the event of a Service failure. PROVIDER MAKES NO

WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE IN CONNECTION WITH THIS AGREEMENT”<sup>18</sup>.

**“Sin garantías<sup>19</sup>.** El proveedor no garantiza que el Servicio se preste sin interrupción. El proveedor no garantiza la calidad ni la puntualidad del Servicio, y no se hará responsable por cualquier pérdida en caso de incumplimiento de Servicios. EL PROVEEDOR NO SE HACE DE NINGUNA GARANTÍA, EXPRESA O IMPLÍCITA, INCLUYENDO GARANTÍAS DE COMERCIALIZACIÓN U OPTIMIZACIÓN PARA UN PROPÓSITO EN PARTICULAR EN RELACIÓN CON ESTE ACUERDO.”

Pero esto no representa ningún problema al fin y al cabo. Este tipo de garantías se refieren a los casos en los cuales por ejemplo: una instalación fallida o un error en un disco duro produzcan una pérdida de información a la entidad que posee el servidor; y ésta luego demande a la organización que produce el SO por daños y/o perjuicios.

En general, por no decir todo el *software* libre no tiene garantías de ningún tipo para el usuario final, pero este siempre puede contar con los foros de ayuda o líneas de atención al cliente (este tipo de líneas telefónicas sí tienen costo), los cuales ayudan a solucionar todos los problemas con respecto al *software* y *hardware*.

La comunidad de *software* libre es muy unida y colaborativa y no

---

<sup>18</sup> "Licencia del *ClarkConnect* 4.2. "Terms of Service" [en línea].

[http://www.ClarkConnect.com/about/tos\\_pcn.php](http://www.ClarkConnect.com/about/tos_pcn.php)

<sup>19</sup> N. del A.: Esta es una traducción hecha por mí del párrafo en inglés.

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar discriminan por la falta de conocimientos o ignorancia. Así que este tipo de soporte técnico es de mucha utilidad para el usuario final, porque el *software* libre da la posibilidad de transmitir conocimientos a cualquiera y estos conocimientos son los que ayudan a solucionar los problemas o dudas y esto se esparce por todo el Internet sin costo alguno.

## **4.2 PREPARATIVOS**

Qué se necesita para poder instalar un *GNU/Linux ClarkConnect 4.2*:

1. Un equipo al que se le pueda dedicar totalmente la tarea de *Servidor/Firewall*.
2. Una conexión a Internet, preferiblemente Banda Ancha (mínimo 512 kbps) o *ADSL*<sup>20</sup>.
3. Una red de área local (*LAN*), en este caso no importa el tamaño aunque entre más terminales se encuentren conectadas a la red se debe considerar instalar más servidores a lo largo de *LAN* según su topología.
4. Un CD conteniendo la imagen de disco de *ClarkConnect 4.2 Community*.

---

<sup>20</sup> Siglas de *Asymmetric Digital Subscriber Line*

5. Es opcional, pero es bueno tener en cuenta donde se ubicará el *Servidor/Firewall*, se recomienda tenerlo cerca del punto de acceso a Internet para poderlo conectar directamente al módem de Internet.

### **4.3 REQUERIMIENTOS**

Los requerimientos de sistema son las características que el *hardware* debe tener como mínimo según la finalidad y el tipo de uso del *Servidor/Firewall*.

**Nota:** el servidor *ClarkConnect* no necesita teclado ni monitor después de su instalación y configuración.

**Tabla 3 - Requerimientos mínimos**

<b>Hardware Base</b>	
<u>Procesador/ CPU</u>	Hasta cuatro procesadores - <i>Pentium®</i> , <i>Celeron®</i> , <i>AMD Athlon®</i>
<u>Memoria RAM</u>	Como mínimo se recomienda 512 MB
<u>Disco duro</u>	Como mínimo se recomienda 1 GB de almacenamiento
<u>Unidad óptica/ CD-ROM</u>	Se requiere únicamente para la instalación
<u>Tarjeta video</u>	Cualquier tarjeta de video
<u>Unidad de Floppy</u>	No es requerida
<u>Tarjeta de sonido</u>	No es requerida
<b>Periféricos</b>	
<u>Mouse</u>	No es requerido
<u>Monitor y teclado</u>	Sólo requerido para la instalación
<b>Red</b>	
<u>Conexión a Internet (Broadband)</u>	<i>Ethernet</i> , banda ancha , <i>DSL</i> o conexión <i>wireless</i>
<u>Tarjetas (adaptadores) de red</u>	<i>PCI</i> , <i>ISA</i> o <i>PCMCIA Wireles</i>

Directrices de hardware:

Estas son guías para estimar que tipo de *hardware* se requiere para el sistema. Es necesario tener en cuenta que el *hardware* requerido depende de cómo se use el *software*. Por ejemplo, un uso continuo del filtro de contenido necesita más poder de cómputo que un sistema que corre un simple *Firewall*.

**Tabla 4 - Directrices de hardware**

<b>RAM y CPU</b>	<b>&lt;5 usuarios</b>	<b>5-10 usuarios</b>	<b>10-50 usuarios</b>	<b>50-200 usuarios</b>
<u>Procesador/ CPU</u>	500 MHz	1 GHz	2 GHz	3 GHz
<u>Memoria RAM</u>	512 MB	1 GB	1.5 GB	2 GB
<b>Disco duro</b>				
<u>Disco duro</u>	La instalación y <i>logs</i> requieren 1 GB, almacenamiento adicional depende del usuario.			

Estos requerimientos arriba mostrados son sólo guías para el usuario y son los recomendados por *ClarkConnect (Point Clark Networks)*. El usuario final es el que decide que tipo de sistema prefiere disponer.

### **4.3.1 HARDWARE A IMPLEMENTAR**

Llegó el momento de afrontar el proyecto informático y escoger el *hardware* que se ejecutará en los equipos, hay muchas cosas que se deben tener en cuenta para esto, como por ejemplo: el procesador y la memoria, dos de los recursos mas críticos en un servidor. Las posibilidades en la selección del *hardware* son prácticamente infinitas, el resultado de esto es la complejidad que se presenta para entender las implicaciones que representa seleccionar una alternativa de otra.

- ¿Qué alternativa posee un balance entre necesidades y costos de implantación y mantenimiento?
- ¿Cuán fiable es cada solución?

Este tipo de preguntas son las que juntas ayudan a tomar la decisión final en la selección del *hardware*.

Se debe entender la informática como un medio, no un fin; se buscan soluciones prácticas, adaptables, funcionales y que no presenten problemas al mejor costo.

De ahí parten las mejores virtudes del *open source*: simple, adaptable, fiable y de bajo costo.

A continuación presento dos opciones en *hardware* para la instalación del Servidor/*Firewall*.

### 4.3.2 OPCIÓN 1:

Esta primera opción consta de un equipo de marca *Hewlett-Packard (HP)* diseñado para emplearse como servidor, lo cual es una ventaja en cuestión de desempeño. Es un equipo nuevo donde se le instalaría el “*ClarkConnect 4.2*” para su función como *Servidor/Firewall*.

Adicionalmente se incluye una tarjeta de red de 10/100/1000, la cual es necesaria para el funcionamiento del *Firewall*, ésta tiene un precio de US\$ 12,00.

**Tabla 5 - Componentes servidor opción 1**

<b>HP ML110 G4</b>	
Procesador/ <i>CPU</i>	<i>Intel® DUAL CORE 925 (3,0 GHz, 2MB caché 800 MHZ FSB)</i>
<u>Memoria RAM</u>	2 GB. PC2-5300 ECC (DDR2-667Mhz), máximo 8 GB
<u>Disco duro</u>	1x160GB SATA
<u>Unidad óptica/ CD-ROM</u>	Incluida
<u>Tarjeta video</u>	Incluida, genérica
<u>Controlador de red</u>	<i>Embedded (integrado) NC320i</i> 10/100/1000

Valor: US\$ 1.040,00\*.

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

\*El valor es aproximado y puede variar en cualquier momento. Este valor proviene de la cotización realizada el 19 de marzo de 2008 en “Sistema Binario Ltda.” ubicado en la dirección: Diagonal 43 B 5 A 13 Oficina 207, Patio Bonito, Medellín.

### **4.3.3 OPCIÓN 2:**

En esta segunda opción, el *Servidor/Firewall* es un equipo que la institución posee, al cual no se le tiene uso en la actualidad. Es un equipo de escritorio que puede tomar el papel de servidor. Sus ventajas son el tamaño pequeño que posee y el precio: ninguno\*\*; igualmente este equipo puede correr sin dificultad el *ClarkConnect 4.2*.

**Tabla 6 - Componentes servidor opción 2**

<b>PC de escritorio</b>	
Procesador/ <i>CPU</i>	<i>Intel</i> ®
Memoria <i>RAM</i>	256 MB , máximo 512 MB
<u>Disco duro</u>	Falta
<u>Unidad óptica/CD-ROM</u>	Falta
<u>Tarjeta video</u>	Incluida, genérica
<u>Controlador de red</u>	1. Incluido 10/100 2. <i>D-Link</i> 10/100

Valor: ninguno\*\*

Se sugiere aumentar al máximo la memoria *RAM* para aumentar así la capacidad del servidor.

\*\*El equipo en sí no tiene ningún costo, los costos adicionales los traen un disco duro y la unidad óptica/*CD-ROM* que le faltan.

## 4.4 COMPATIBILIDAD

Normalmente *Linux* tiene un buen soporte para el *hardware* y entre este mas popular sea mejor soporte tendrá. Para evitar futuros problemas con el *hardware*, este debe ser seleccionado para que sea preferiblemente 100% compatible con *Linux*. Escoger un vendedor de servidores como *HP* es un punto a tener en cuenta, ya que ellos venden algunos de sus servidores con *Red Hat Enterprise Linux*<sup>21</sup> pre-instalado y es una gran ventaja porque el *hardware* soportado por *Red Hat Linux* es el soportado por el *ClarkConnect*. Para consultas sobre *hardware* compatible se puede mirar la *Red Hat Compatibility Guide* en <https://hardware.redhat.com/hwcert/index.cgi>.

Por otro lado, *ClarkConnect* no tiene dificultad al conectarse a Internet en Colombia.

---

<sup>21</sup> Distribución *Linux* de tipo comercial muy popular entre las empresas. Creada y mantenida por la compañía del mismo nombre. Sus programadores han contribuido a la comunidad libre con varias tecnologías y *software*.

## 4.5 INSTALACIÓN

En esta sección veremos cómo se realiza la instalación del *ClarkConnect* 4.2 paso a paso.

Es necesario poder arrancar (“bootear<sup>22</sup>”) el servidor por *CD-ROM*. Si esta opción no está habilitada, en las opciones de la *BIOS*<sup>23</sup> se debe modificar el orden de arranque de las unidades para que la unidad de *CD-ROM* sea la primera seguida del disco duro primario.

Para ello se prende el equipo, durante el encendido este muestra la pantalla de la *BIOS*, la cual nos brinda algunas opciones, una de estas se llama *Setup* o similar, también es posible que aparezca indicación del estilo "pres DEL to enter setup". Normalmente se ingresa a esta sección presionando la tecla F2, Esc o Supr. Este mensaje solo aparece por poco tiempo, por ello se sugiere presionar repetidamente la tecla para ingresar al menú de la *BIOS*.

Dentro del menú de la *BIOS*, buscamos una sección llamada *Boot* o *Advanced BIOS Features*, para llegar allí empleamos los cursores y la tecla *Enter*. Dentro se debe buscar un sub-menú parecido a *Boot Sequence* o *First Boot Device*. Nos paramos en el sub-menú y lo organizamos de forma tal que el primer dispositivo de arranque (“booteo”) sea la unidad óptica/*CD-ROM*. Para ello se usa las teclas +/- o

---

22 Término que se refiere a modificar el arranque de los dispositivos de almacenamiento para iniciar con él en primer lugar.

23 *Basic Input-Output System*, sistema básico de entrada-salida. *Software* básico instalado en la placa base o tarjeta madre que inicia el SO.

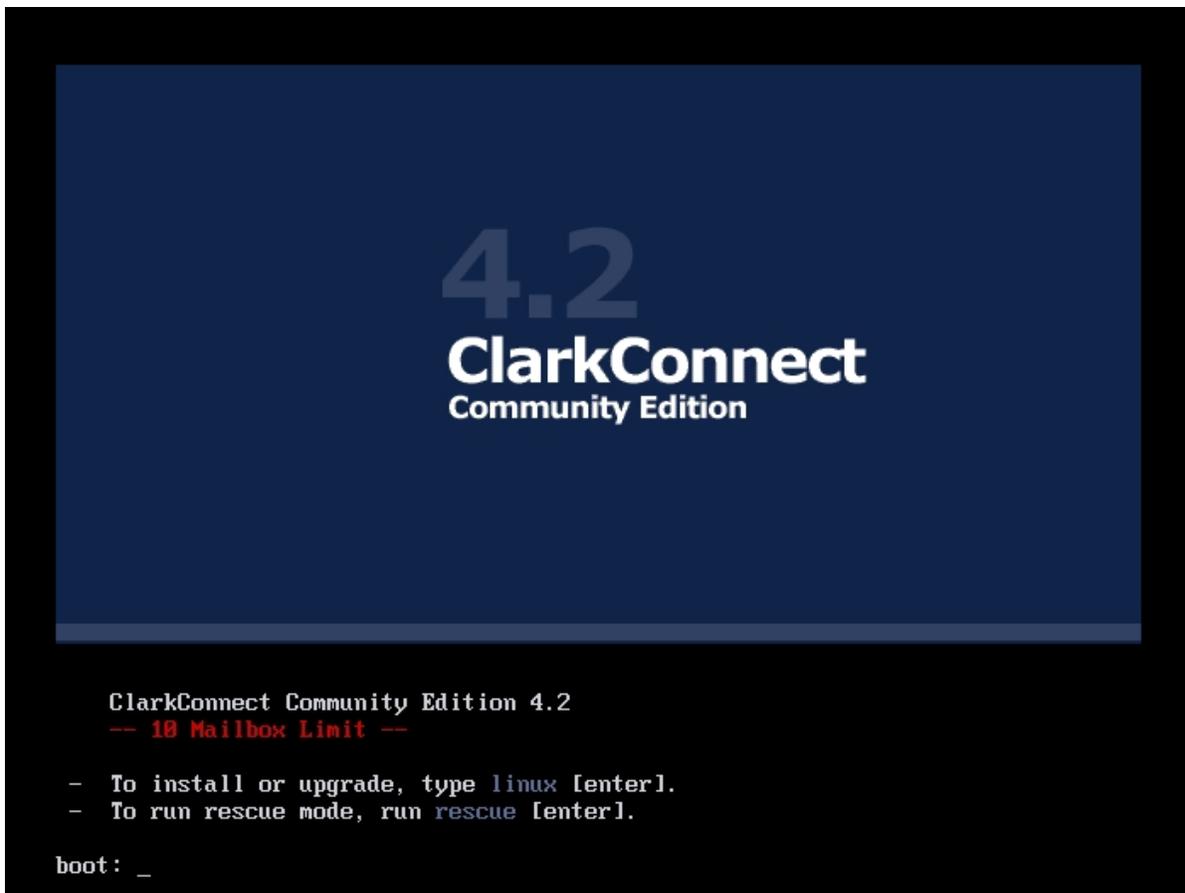
Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

Av. *Pag.Pag.* / Reg. *Pag.* . Una vez realizados los cambios estos se deben guardar, para ello presionamos `Esc` o buscamos un menú similar a *Exit* y presionamos en la opción `Exit and Saving Changes`. Después de esto el equipo debe reiniciar y podremos iniciar con *CD-ROM* sin problemas.

**Nota:** Al terminar la instalación todo el contenido que hubiera en el disco duro habrá sido borrado y una recuperación de estos datos es poco probable.

## 4.5.1 CONFIGURANDO PARA INSTALAR

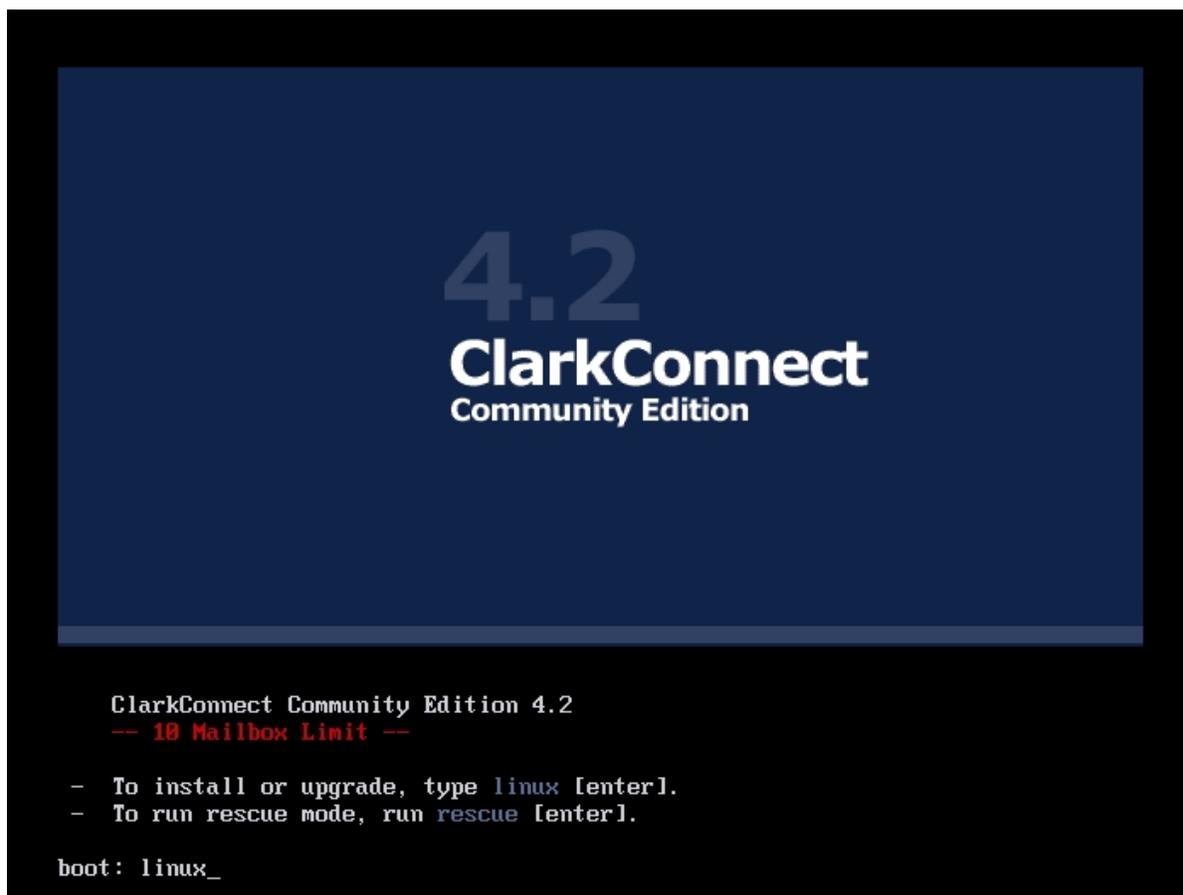
[Imagen 1]



Después de encender el servidor e introducir el *CD* de instalación aparecerá la pantalla de bienvenida. Aquí nos pide introducir `linux` para instalar o `rescue` para recuperar una instalación fallida del

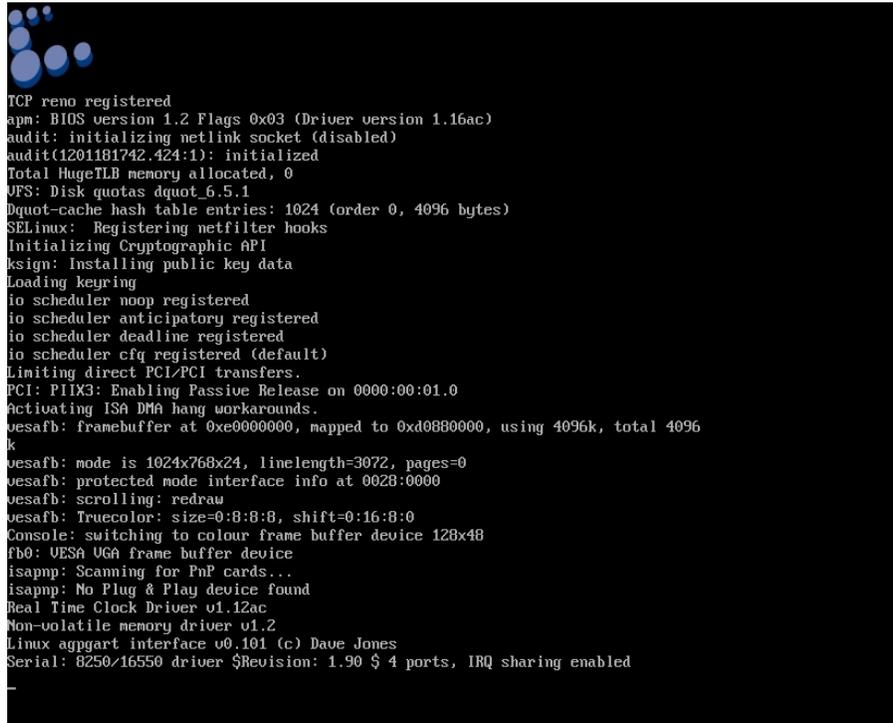
Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar servidor. En nuestro caso nos interesa instalar el *ClarkConnect*, así que escribimos `Linux` y presionamos `Enter`.

[Imagen 2]



Esto nos lleva a una ventana donde se descarga el sistema base del *CD-ROM* a la memoria *RAM*. Estos datos no son relevantes para nosotros en este momento. No tenemos que hacer más que esperar a que cargue y comience el asistente de instalación (*installation wizard*).

[Imagen 3]



```
TCP reno registered
apm: BIOS version 1.2 Flags 0x03 (Driver version 1.16ac)
audit: initializing netlink socket (disabled)
audit(1201181742.424:1): initialized
Total HugeTLB memory allocated, 0
VFS: Disk quotas dquot_6.5.1
Dquot-cache hash table entries: 1024 (order 0, 4096 bytes)
SELinux: Registering netfilter hooks
Initializing Cryptographic API
ksign: Installing public key data
Loading keyring
io scheduler noop registered
io scheduler anticipatory registered
io scheduler deadline registered
io scheduler cfq registered (default)
Limiting direct PCI/PCI transfers.
PCI: PIIX3: Enabling Passive Release on 0000:00:01.0
Activating ISA DMA hang workarounds.
vesafb: framebuffer at 0xe0000000, mapped to 0xd0880000, using 4096k, total 4096k
vesafb: mode is 1024x768x24, linelength=3072, pages=0
vesafb: protected mode interface info at 0028:0000
vesafb: scrolling: redraw
vesafb: Truecolor: size=0:8:8:8, shift=0:16:8:0
Console: switching to colour frame buffer device 128x48
fb0: UESA VESA VGA frame buffer device
isapnp: Scanning for PnP cards...
isapnp: No Plug & Play device found
Real Time Clock Driver v1.12ac
Non-volatile memory driver v1.2
Linux agpgart interface v0.101 (c) Dave Jones
Serial: 8250/16550 driver $Revision: 1.90 $ 4 ports, IRQ sharing enabled
```

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 4]

```
opn: BIOS version 1.2 Flags 0x03 (Driver version 1.16ac)
audit: initializing netlink socket (disabled)
audit(1201481742.424:1): initialized
Total HugeTLB memory allocated, 0
VFS: Disk quotas dquot_6.5.1
Dquot-cache hash table entries: 1024 (order 0, 4096 bytes)
SELinux: Registering netfilter hooks
Initializing Cryptographic API
ksign: Installing public key data
Loading keyring
io scheduler noop registered
io scheduler anticipatory registered
io scheduler deadline registered
io scheduler cfq registered (default)
Limiting direct PCI/PCI transfers.
PCI: PIIX3: Enabling Passive Release on 0000:00:01.0
Activating ISA DMA hang workarounds.
vesafb: framebuffer at 0xe0000000, mapped to 0xd0880000, using 4096k, total 4096k
vesafb: mode is 1024x768x24, linelength=3072, pages=0
vesafb: protected mode interface info at 0028:0000
vesafb: scrolling: redraw
vesafb: Truecolor: size=0:8:8:0, shift=0:16:8:0
console: switching to colour frame buffer device 120x40
fb0: UESA VGA frame buffer device
isapnp: Scanning for PnP cards...
isapnp: No Plug & Play device found
Real Time Clock Driver v1.12ac
Non-volatile memory driver v1.2
Linux agpgart interface v0.101 (c) Dave Jones
Serial: 8250/16550 driver $Revision: 1.90 $ 4 ports, IRQ sharing enabled
serial8250: ttyS0 at I/O 0x3f8 (irq = 4) is a 16450
PDC 0 is a SB2078B
RAMDISK driver initialized: 16 RAM disks of 16384K size 1024 blocksize
Uniform Multi-Platform E-IDE driver Revision: 7.00alpha2
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PIIX3: IDE controller at PCI slot 0000:00:01.1
PIIX3: chipset revision 0
PIIX3: not 100% native mode: will probe irqs later
   ide0: BM-DMA at 0xc000-0xc007, BIOS settings: hda:pio, hdb:pio
   ide1: BM-DMA at 0xc008-0xc00f, BIOS settings: hdc:pio, hdd:pio
hda: QEMU HARDDISK, ATA DISK drive
```

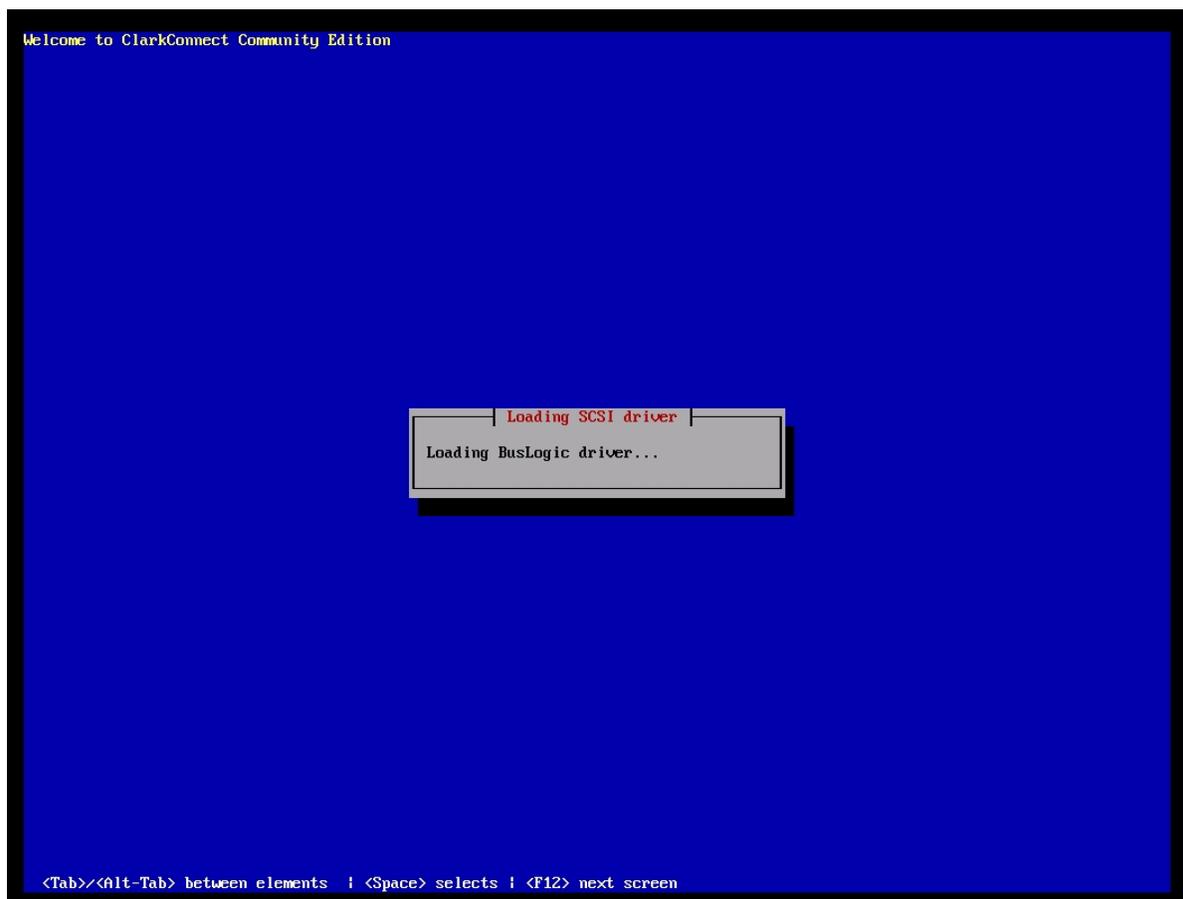
[Imagen 5]

```
audit(1201101742.424:1): Initialized
Total HugeTLB memory allocated, 0
UFS: Disk quotas dqquot 6.5.1
Dquot-cache hash table entries: 1024 (order 0, 4096 bytes)
SELinux: Registering netfilter hooks
Initializing Cryptographic API
ksign: Installing public key data
Loading keyring
io scheduler noop registered
io scheduler anticipatory registered
io scheduler deadline registered
io scheduler cfq registered (default)
Limiting direct PCI/PCI transfers.
PCI: PIIX3: Enabling Passive Release on 0000:00:01.0
Activating ISA DMA hang workarounds.
vesafb: framebuffer at 0xe0000000, mapped to 0xd0880000, using 4096k, total 4096k
vesafb: mode is 1024x768x24, linelength=3072, pages=0
vesafb: protected mode interface info at 0028:0000
vesafb: scrolling: redraw
vesafb: Truecolor: size=0:8:8:8, shift=0:16:8:0
Console: switching to colour frame buffer device 128x48
fb0: UESA VGA frame buffer device
isapp: Scanning for PnP cards...
isapp: No Plug & Play device found
Real Time Clock Driver v1.12ac
Non-volatile memory driver v1.2
Linux agpgart interface v0.101 (c) Dave Jones
Serial: 8250/16550 driver $Revision: 1.90 $ 4 ports, IRQ sharing enabled
serial8250: ttyS0 at I/O 0x3f8 (irq = 4) is a 16450
FDC 0 is a SB207BB
RAMDISK driver initialized: 16 RAM disks of 16384K size 1024 blocksize
Uniform Multi-Platform E-IDE driver Revision: 7.00alpha2
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PIIX3: IDE controller at PCI slot 0000:00:01.1
PIIX3: chipset revision 0
PIIX3: not 100% native mode: will probe irqs later
   ide0: BM-DMA at 0xc000-0xc007, BIOS settings: hda:pio, hdb:pio
   ide1: BM-DMA at 0xc008-0xc00f, BIOS settings: hdc:pio, hdd:pio
hda: QEMU HARDDISK, ATA DISK drive
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
hdc: QEMU CD-ROM, ATAPI CD/DVD-ROM drive
```

[Imagen 6]

```
   ide0: BM-DMA at 0xc000-0xc007, BIOS settings: hda:pio, hdb:pio
   ide1: BM-DMA at 0xc008-0xc00f, BIOS settings: hdc:pio, hdd:pio
hda: QEMU HARDDISK, ATA DISK drive
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
hdc: QEMU CD-ROM, ATAPI CD/DVD-ROM drive
ide1 at 0x1f0-0x1f7,0x3f6 on irq 15
hda: max request size: 512KiB
hda: 6144000 sectors (3145 MB) w/256KiB Cache, CHS=6095/255/63, (U)DMA
hda: cache flushes supported
hda: unknown partition table
ide-floppy driver 0.99.newide
usbcore: registered new driver hiddev
usbcore: registered new driver usbhid
drivers/usb/input/hid-core.c: v2.6:USB HID core driver
RAW: No PS/2 cpmt/hid-core.c: v2.6:USB HID core driver
RAW: No PS/2 controller found. Probing ports directly.
serio: i8042 AUX port at 0x60,0x64 irq 12
serio: i8042 KBD port at 0x60,0x64 irq 1
mice: PS/2 mouse device common for all mice
md: md driver 0.9.3 MAX_MD_DEVS=256, MD_SB_DISKS=27
md: bitmap version 4.39
TCP bic registered
Initializing IPsec netlink socket
NET: Registered protocol family 1
NET: Registered protocol family 17
Using IPI No-Shortcut mode
md: Autodetecting RAID arrays.
time: tsc clocksource has been installed.
md: autorum ...
md: ... autorum DONE.
RAMDISK: Compressed image found at block 0
input: AT Translated Set 2 keyboard as /class/input/input0
UFS: Mounted root (ext2 filesystem).
Greetings.
anaconda installer init version 10.1.1.63 starting
mounting /proc filesystem... done
mounting /dev/pts (unix98 ptty) filesystem... done
mounting /sys filesystem... done
input: ImExPS/2 Generic Explorer Mouse as /class/input/input1
trying to remount root filesystem read write... done
mounting /tmp as ramfs... done
running install...
running /sbin/loader
```

[Imagen 7]

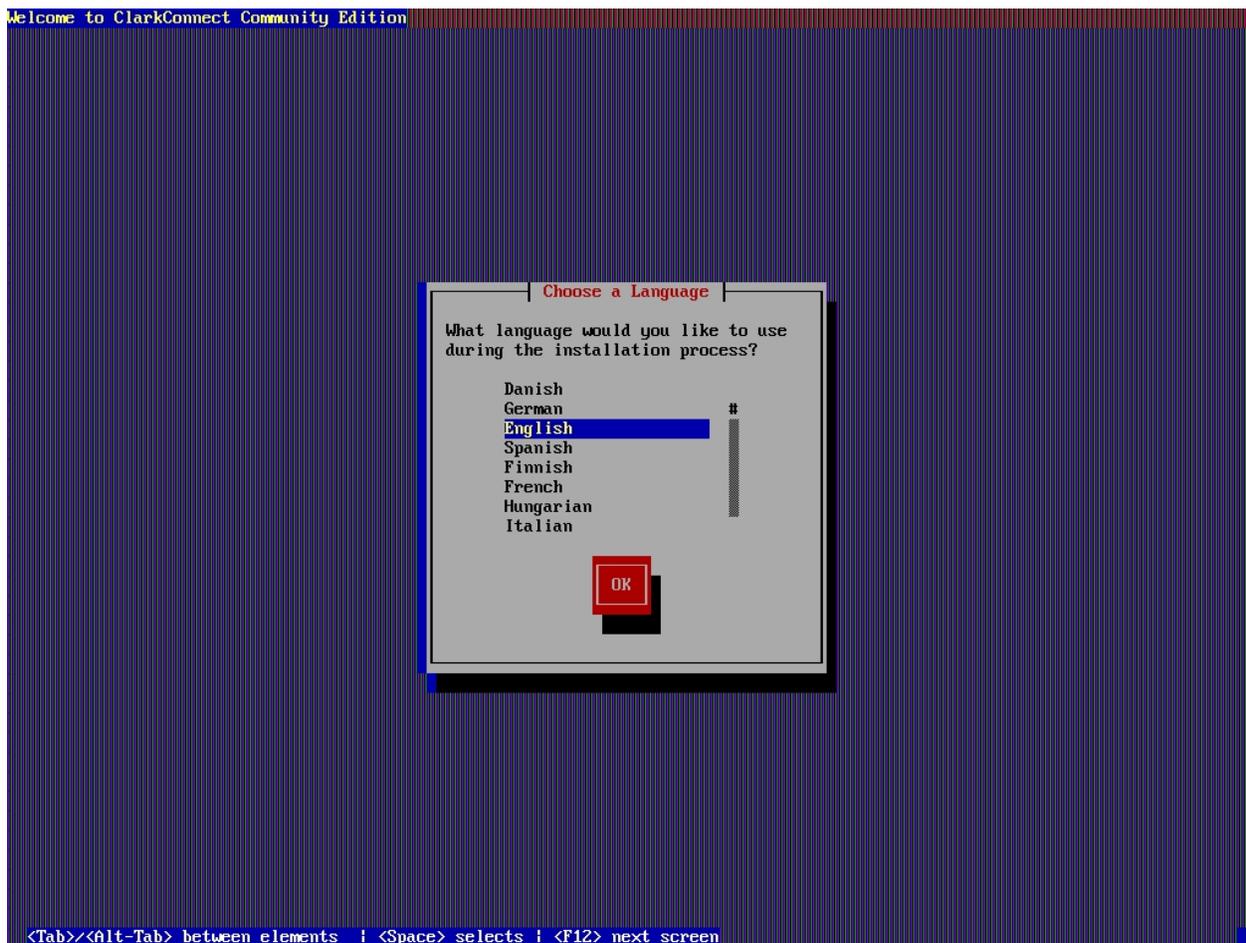


Cuando termine nos preguntará el idioma que queremos utilizar durante la instalación. Pero primero es necesario tener en cuenta con qué teclas se maneja el instalador. En la parte inferior de la pantalla se puede ver una línea azul con las teclas y su descripción:

- -Tab ⇌ para movernos entre los elementos
- -La barra espaciadora (*space bar*) para seleccionar y
- -F12 para continuar en la siguiente ventana

Adicionalmente las teclas de movimiento o cursores ←↑→↓ nos permiten desplazarnos por una lista y sus contenidos, finalmente la tecla *Enter* selecciona nuestra elección.

[Imagen 8]



[Imagen 9]



Volviendo a la instalación nos desplazamos hasta *Spanish*, presionamos *Tab* y luego *Enter*. Esta opción es para escoger el idioma de preferencia durante la instalación y el uso del servidor a través de la interfaz Web<sup>24</sup>.

Es recomendable dejar el lenguaje en inglés, ya que, sólo una pequeña porción del asistente, de instalación al igual que la interfaz

<sup>24</sup>Interfaz (capa de usuario) de un programa accesible desde un navegador. De esta forma se pueden manejar programas, por ejemplo un servidor, a través de una red.

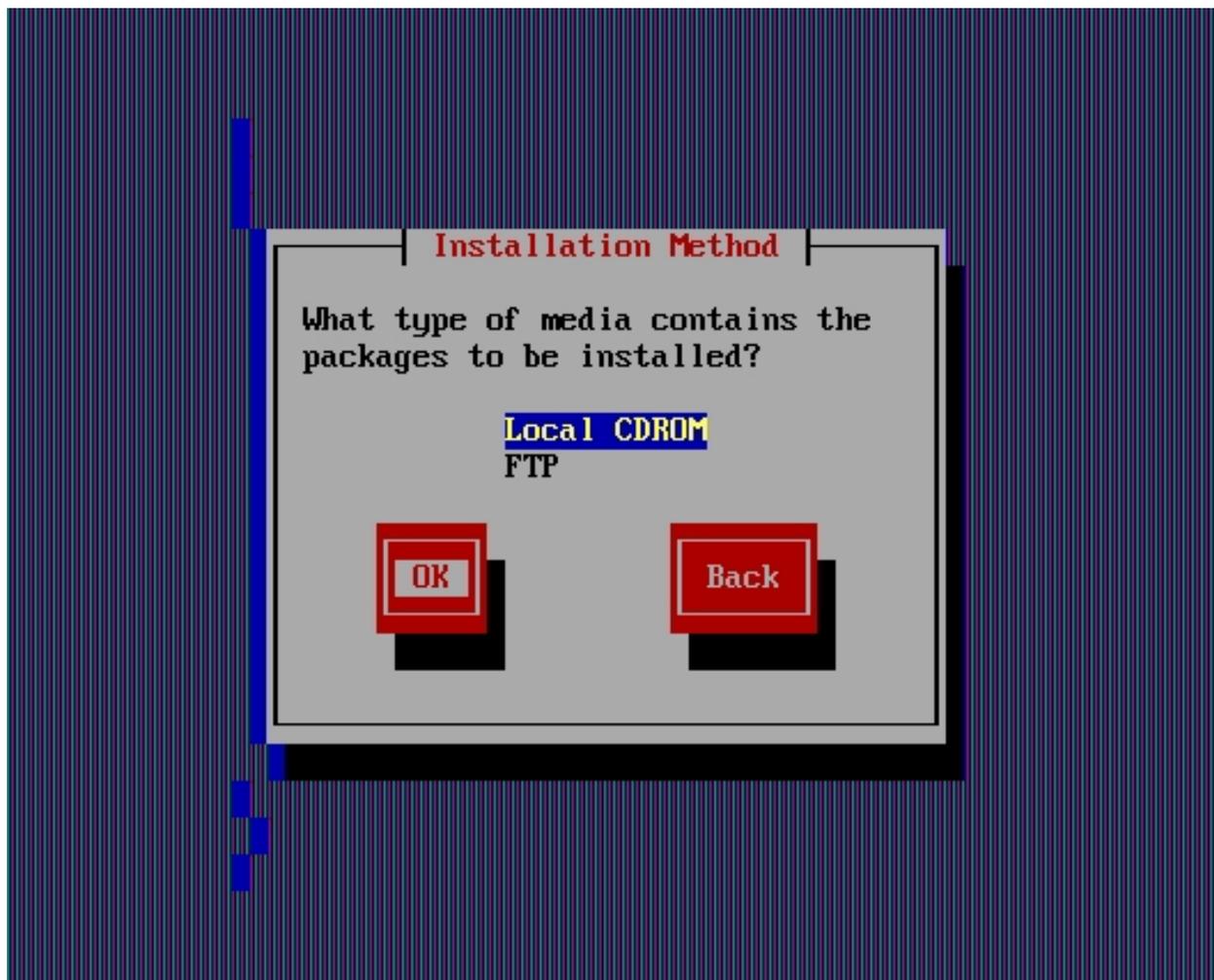
Web, se encuentran traducidos al español. Esto ayuda a evitar confusiones con los idiomas.

[Imagen 10]



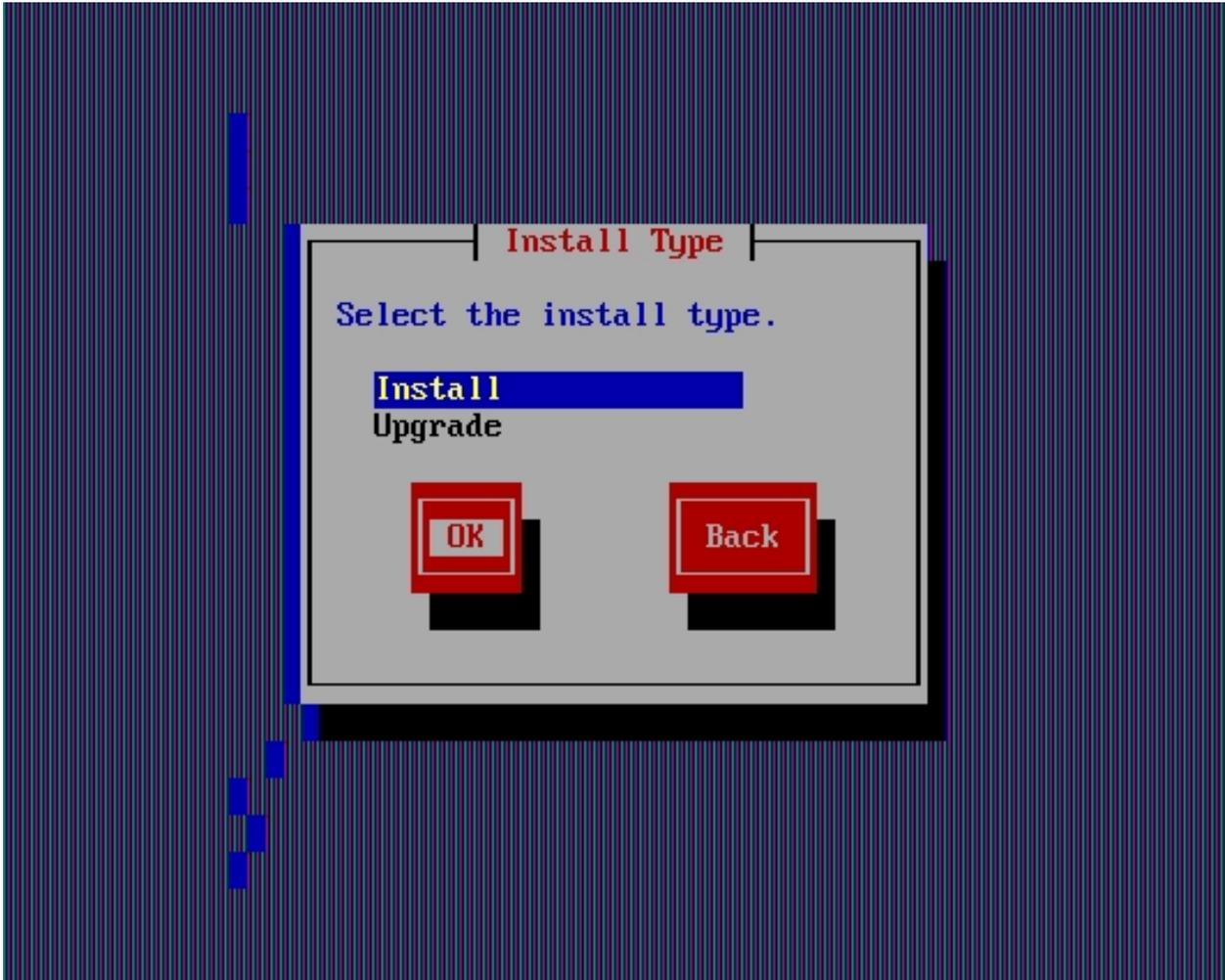
Seleccionamos el tipo de teclado que tenemos, por ejemplo 'us' para el americano y 'es' para el español.

[Imagen 11]



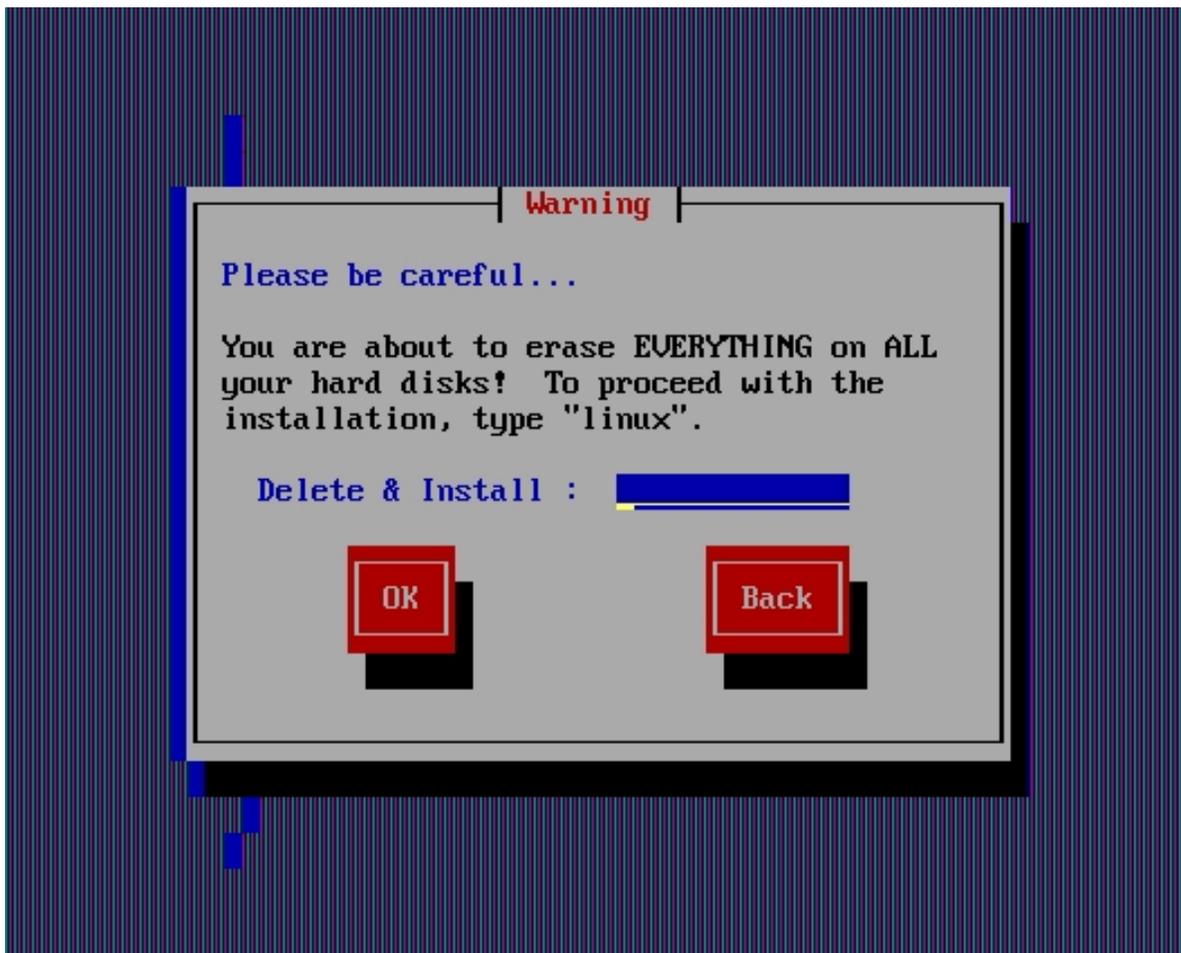
En la siguiente pantalla nos piden escoger el método de instalación. Como hemos descargado la versión completa de la instalación, y ésta se encuentra en el *CD*, nos paramos en la primera opción y la escogemos.

[Imagen 12]



Deseamos instalar así que seleccionamos Install.

[Imagen 13]

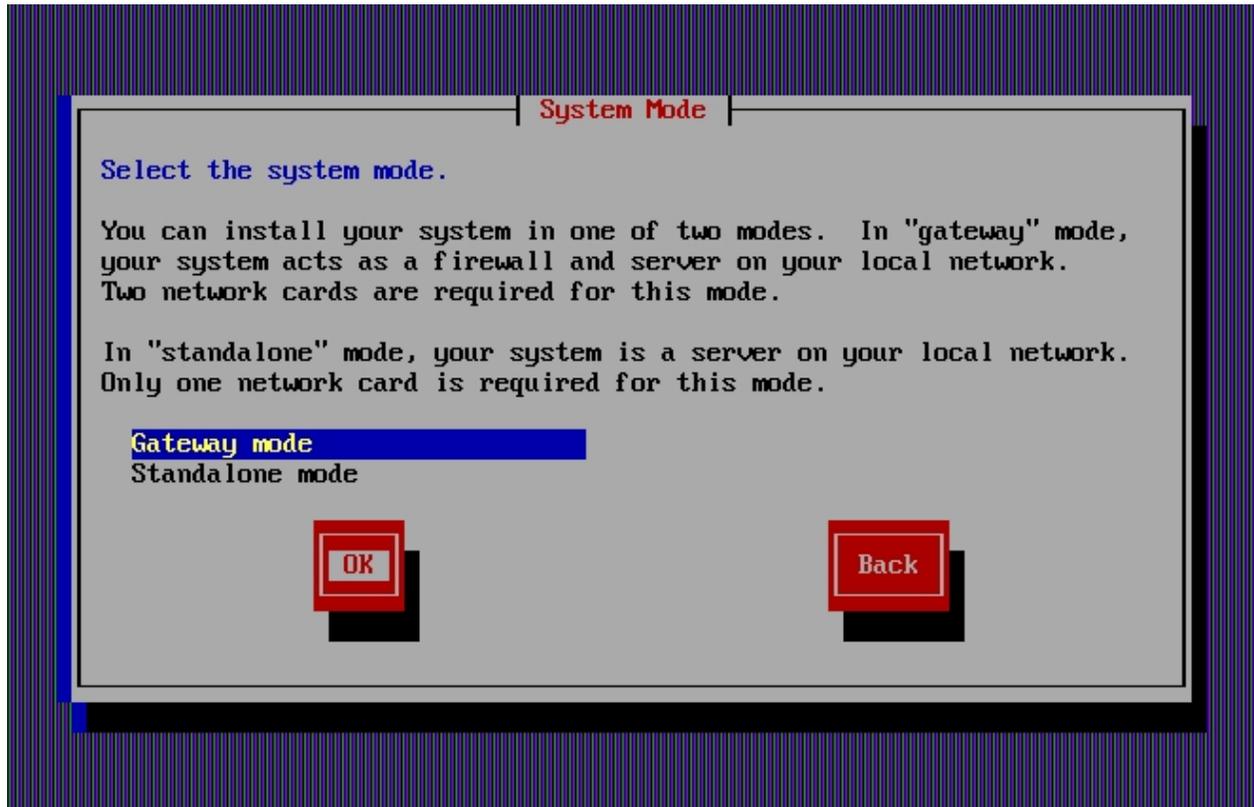


Nos advierten que si continuamos borraremos todo el contenido del disco duro, y nos piden confirmarlo, para ello escribir nuevamente la palabra Linux.

[Imagen 14]

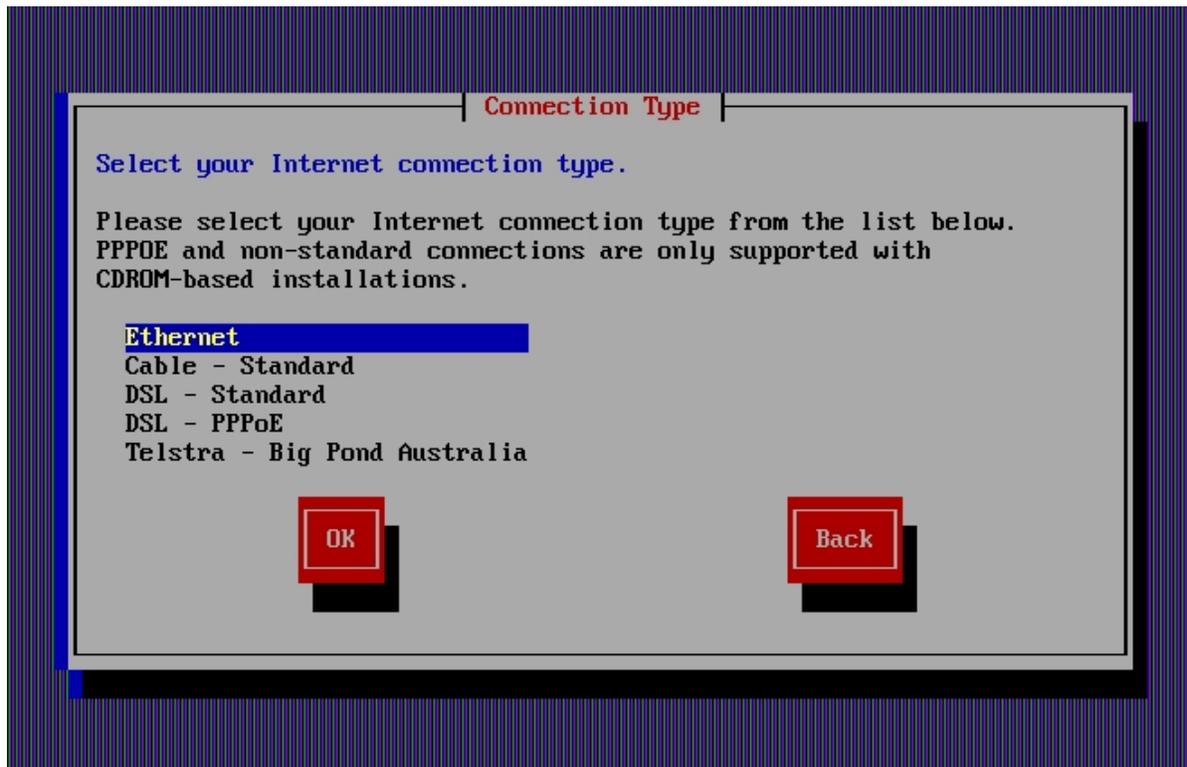


[Imagen 15]



Seleccionando el modo en que se comportará el servidor depende de lo que queramos hacer en él. El *Standalone mode* crea un servidor en una *LAN* detrás de un *Firewall* existente, el servidor entonces tendrá prácticamente todas sus funciones a excepción del *Firewall*, por ejemplo: podrá ser un servidor de archivos. La otra opción *Gateway mode* es la que nos interesa, ya que podemos contar con todo los módulos y posibilidades que nos trae el *ClarkConnect 4.2* y lo mas importante: filtrará el contenido y nos protegerá la *LAN*.

[Imagen 16]

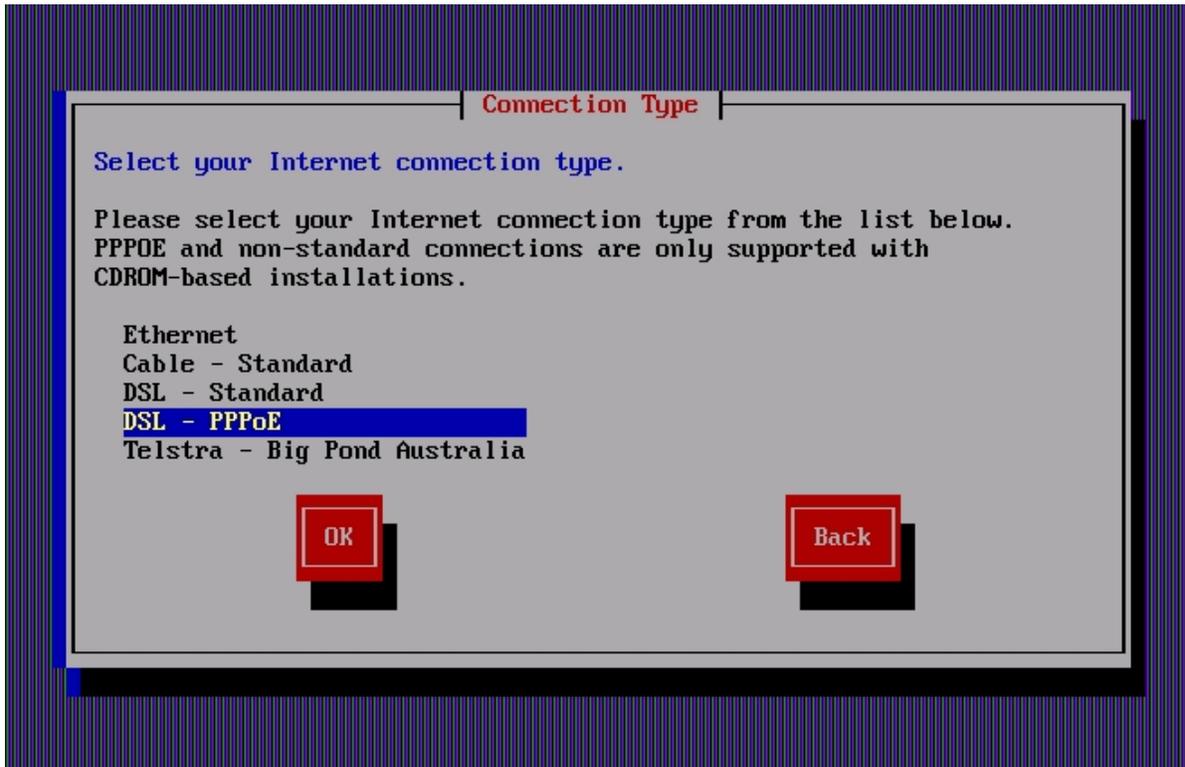


Llegamos a la sección donde debemos seleccionar qué tipo de conexión a Internet tenemos. Dado que el Colegio tiene una conexión tipo *PPPoE*<sup>25</sup> (*Point-to-Point Protocol over Ethernet* o Protocolo Punto a Punto sobre *Ethernet*), seleccionamos esta.

---

<sup>25</sup> *PPPoE* (*Point-to-Point Protocol over Ethernet* o Protocolo Punto a Punto sobre *Ethernet*) es un protocolo de red. Se utiliza comúnmente para proveer conexión de banda ancha mediante un cable-módem. Tiene autenticación y cifrado.

[Imagen 17]



En la siguiente pantalla configuramos las opciones de conexión para el protocolo *PPPoE*. Aquí escribimos el nombre de usuario y debajo la contraseña; si es necesario, también escribir el nombre o la dirección de *IP* del servidor *DNS*<sup>26</sup> primario.

---

<sup>26</sup> *Domain Name System*, es un servidor que traduce las peticiones de dominios de los clientes a direcciones *IP* para su uso en la red, funciona también a la inversa. Ejemplo: `google.com --> 72.14.207.99` .

[Imagen 18]

Configure your PPPoE network settings

Some DSL Internet service providers require a username and password to successfully connect. In some cases, you may need to include your FULL network name (e.g. "bob@sympatico.ca" instead of just "bob")

\* Many ISPs will autoconfigure the nameservers.

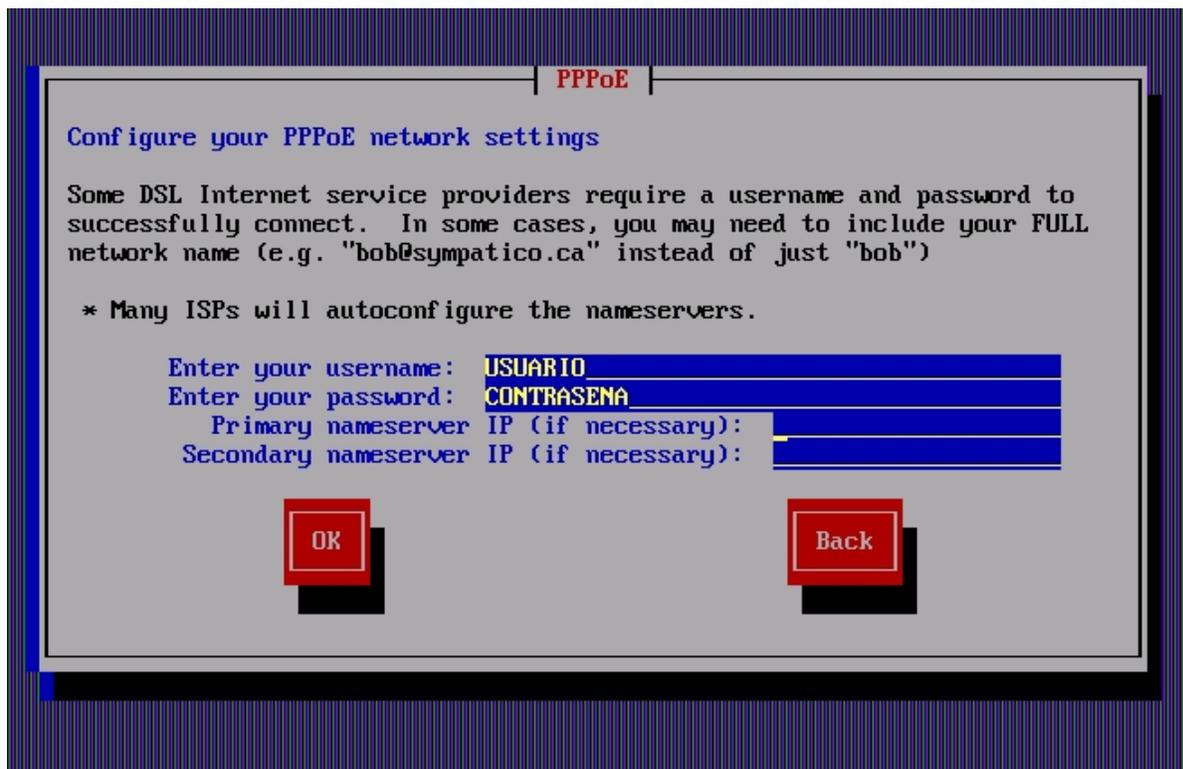
Enter your username:

Enter your password:

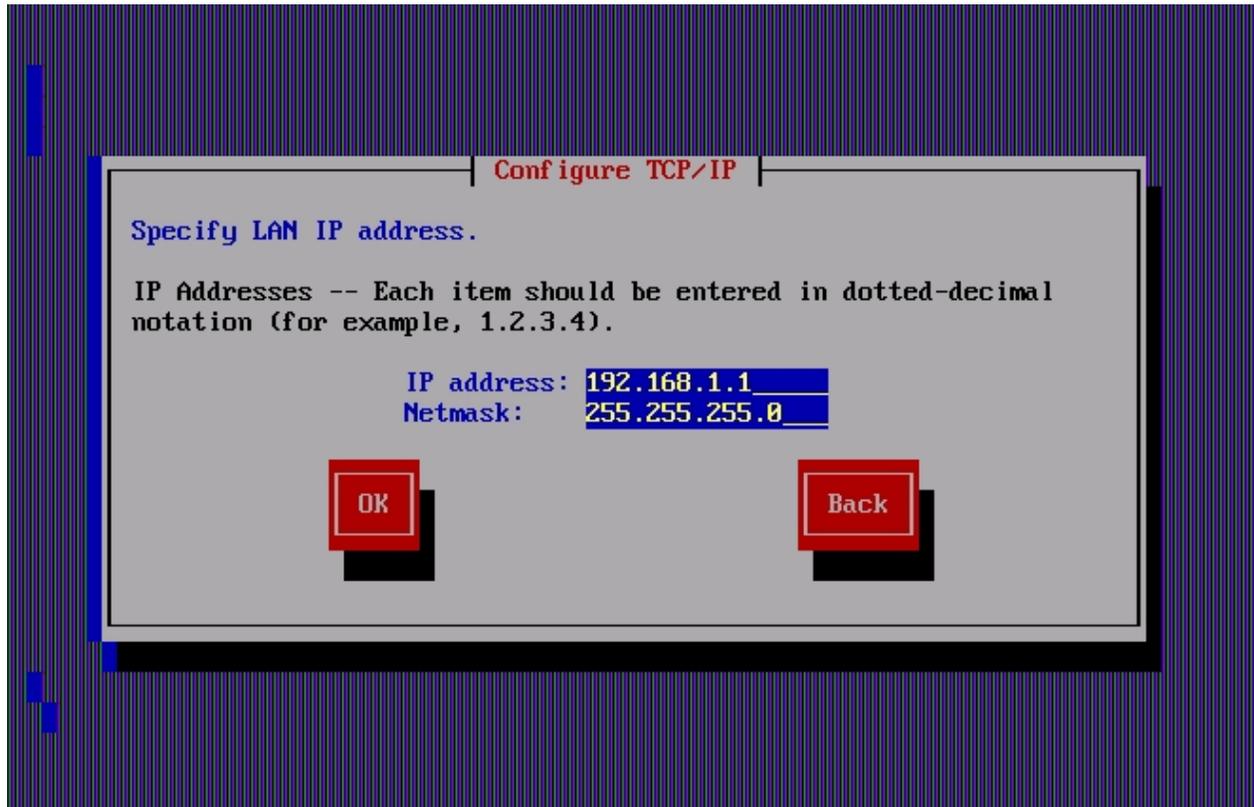
Primary nameserver IP (if necessary):

Secondary nameserver IP (if necessary):

[Imagen 19]



[Imagen 20]



Terminando de configurar la parte de la red, escogemos qué dirección  $IP^{27}$  tendrá nuestro servidor en el dominio. Lo usual son direcciones de este estilo:

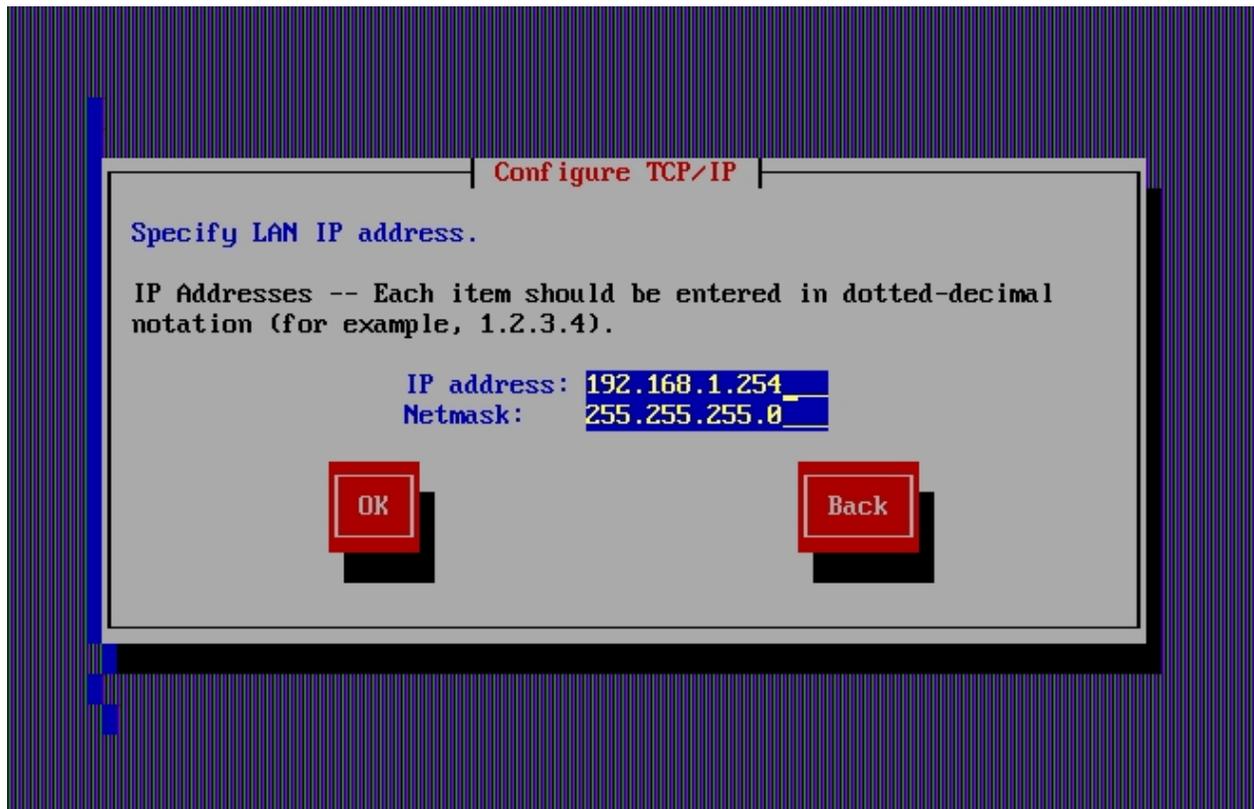
192.168.1.254 o 192.168.50.100

Para los dos últimos números se puede escoger cualquier número en el rango del 0 al 255.

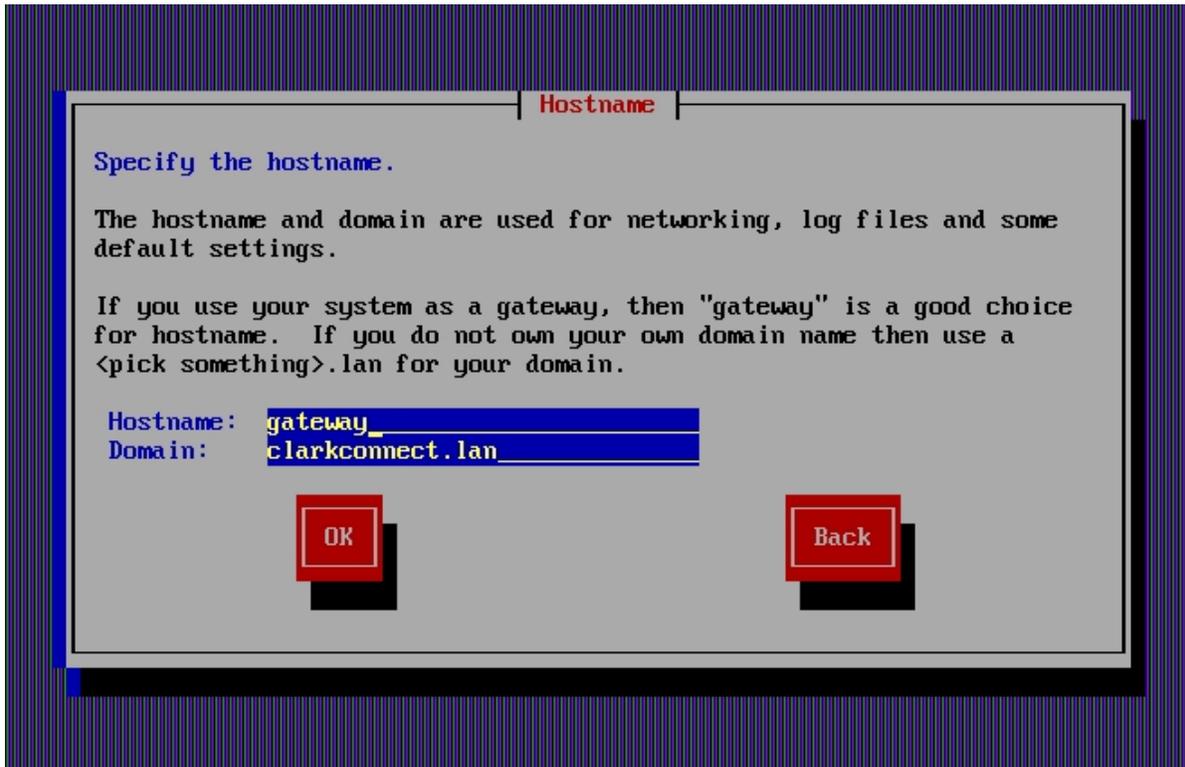
---

<sup>27</sup> Una dirección numérica por la cual se identifica a un sistema en una red, sea local o en Internet.

[Imagen 21]

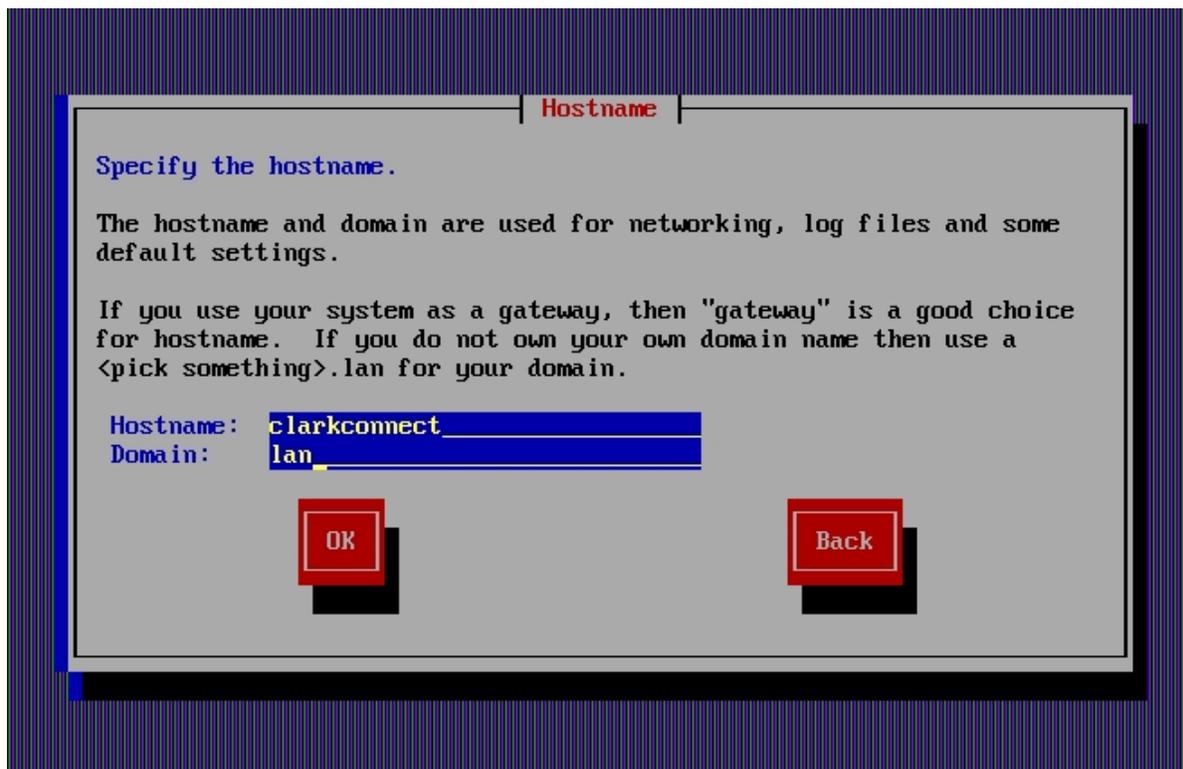


[Imagen 22]

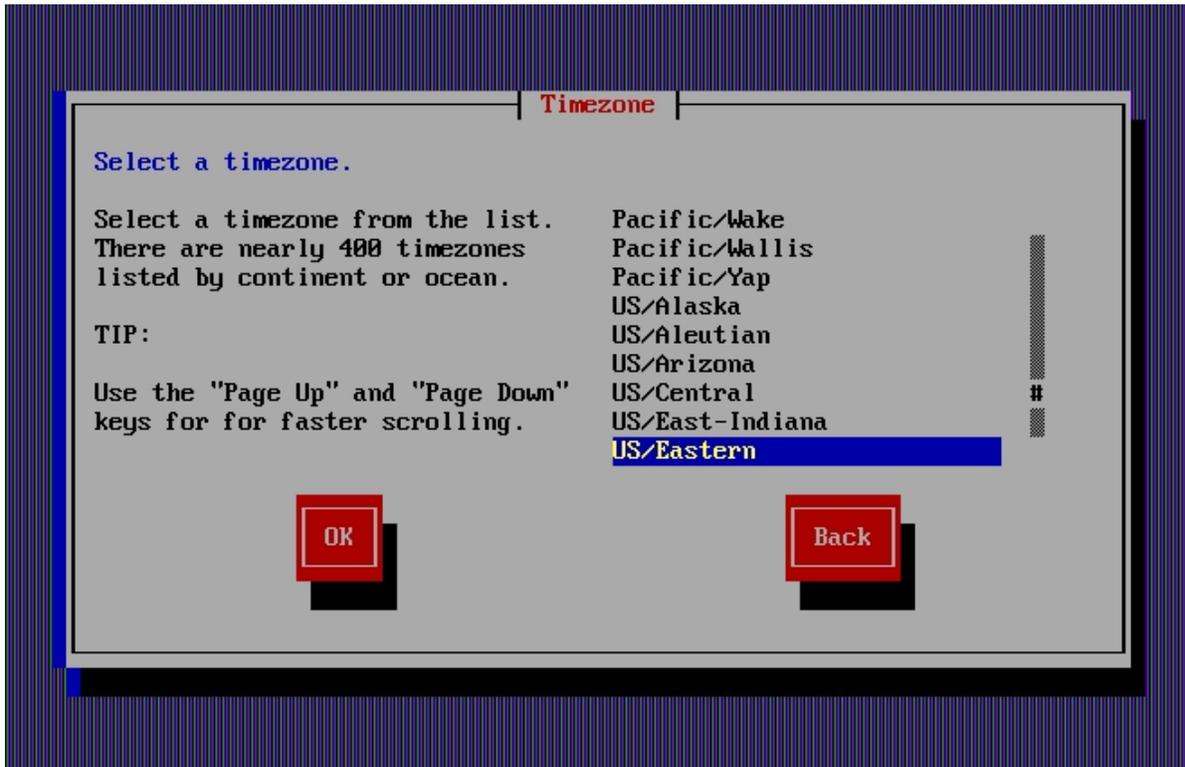


Pasamos a la siguiente ventana y nos encontramos con la opción de elegir el *hostname* (nombre del *host*), que es el nombre que adopta una máquina, por ejemplo un servidor, para ser identificado más fácilmente en una red. Así el administrador de la red no tiene que memorizarse siempre la dirección *IP* de los servidores. Por comodidad se sugiere *ClarkConnect* pero puede ser cualquier otro. Ahora, el dominio es un nombre al cual se le asocian un número de computadores en una red. En este caso el dominio es `colegioalemanmedellin.edu.co`.

[Imagen 23]

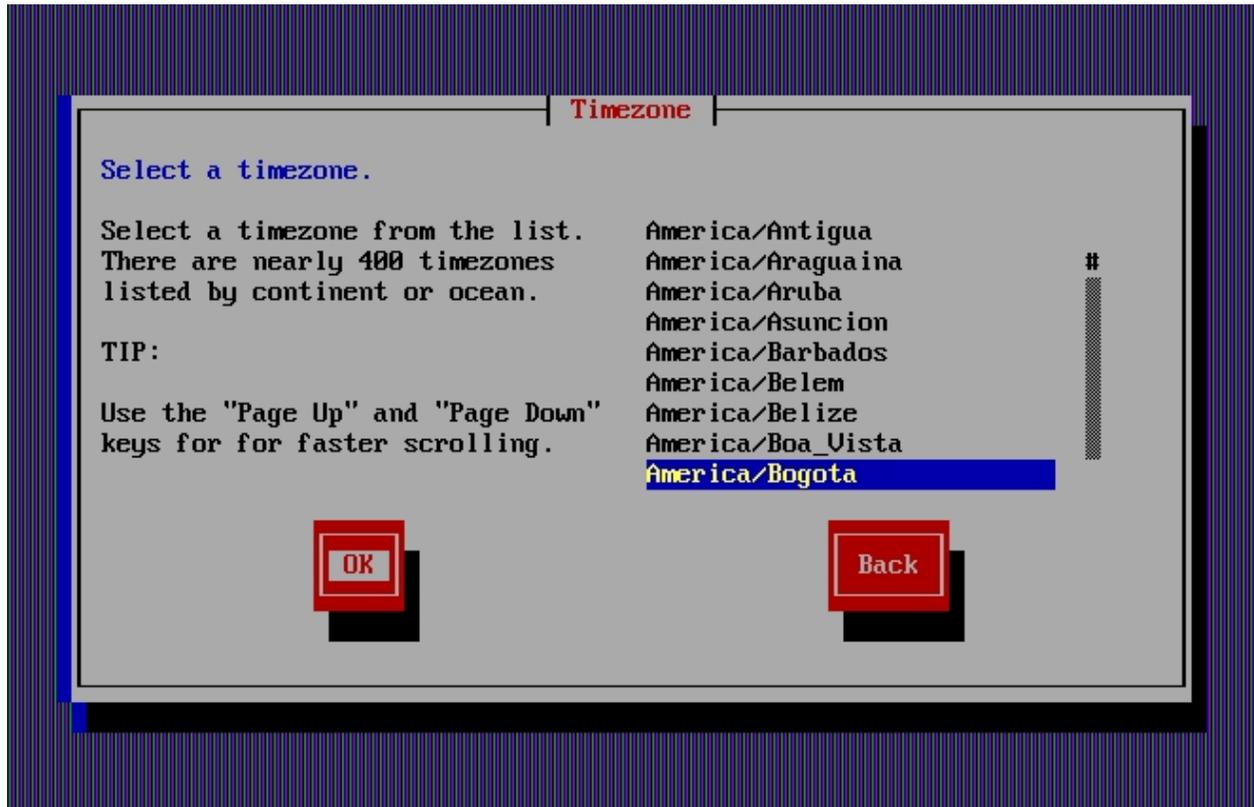


[Imagen 24]

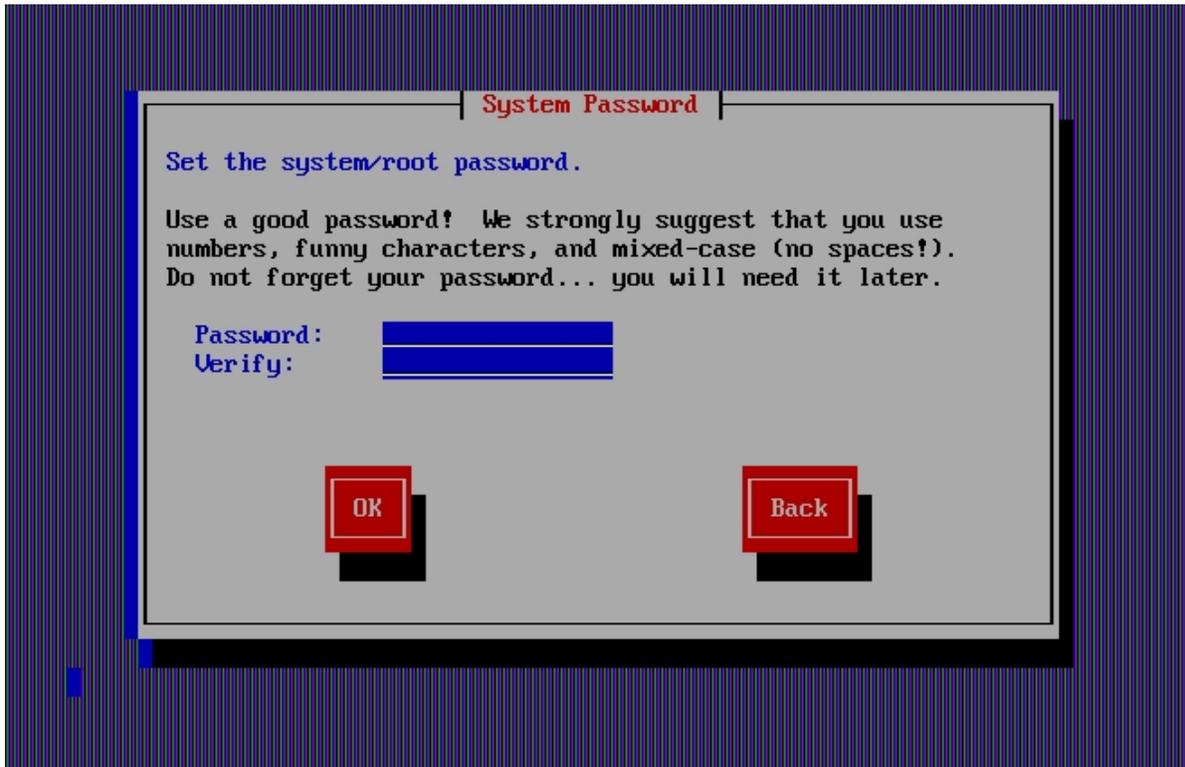


Seleccionar una zona horaria con la ciudad más cercana. Si presionamos 'a' podemos buscar mas fácilmente la zona de América/Bogotá.

[Imagen 25]



[Imagen 26]



Ahora, continuando con la siguiente pantalla, el manual nos pide ingresar una contraseña para el Superusuario<sup>28</sup> (*root*) en el servidor. Es mejor aceptar la sugerencia que nos hacen de usar números, caracteres especiales (ej. : !@#\$%&) y letras en mayúsculas y minúsculas mezcladas entre sí. ¡Y evitar olvidar la contraseña, ya que sin ella nos quedamos sin poder acceder al servidor! Si somos conscientes de la importancia de la seguridad de la información, recomiendo tener una contraseña de 14 caracteres del tipo arriba descrito. De esta forma garantizamos que en los próximos años nadie entre al servidor por fuerza bruta. Podemos disfrazar una frase sencilla con el código de

---

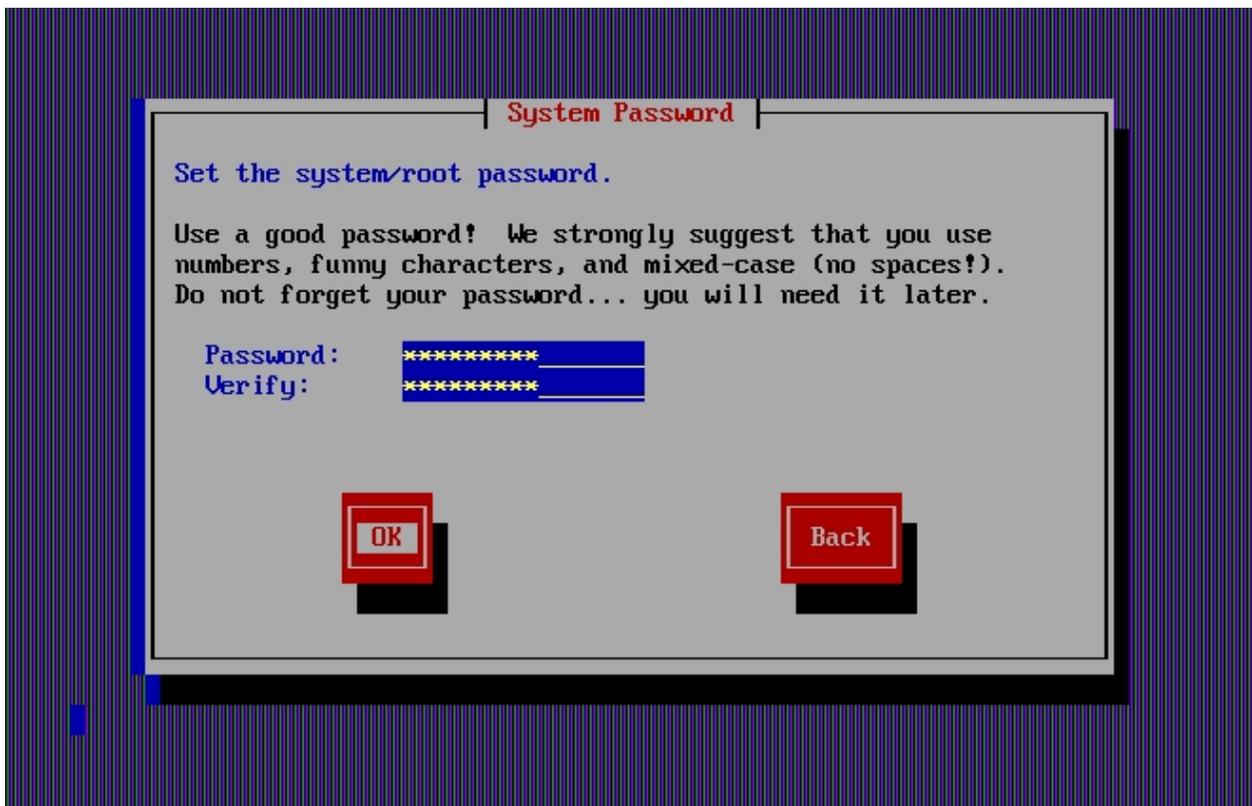
<sup>28</sup> El superusuario o *root* es aquel que administra un sistema *UNIX* o *Linux*.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

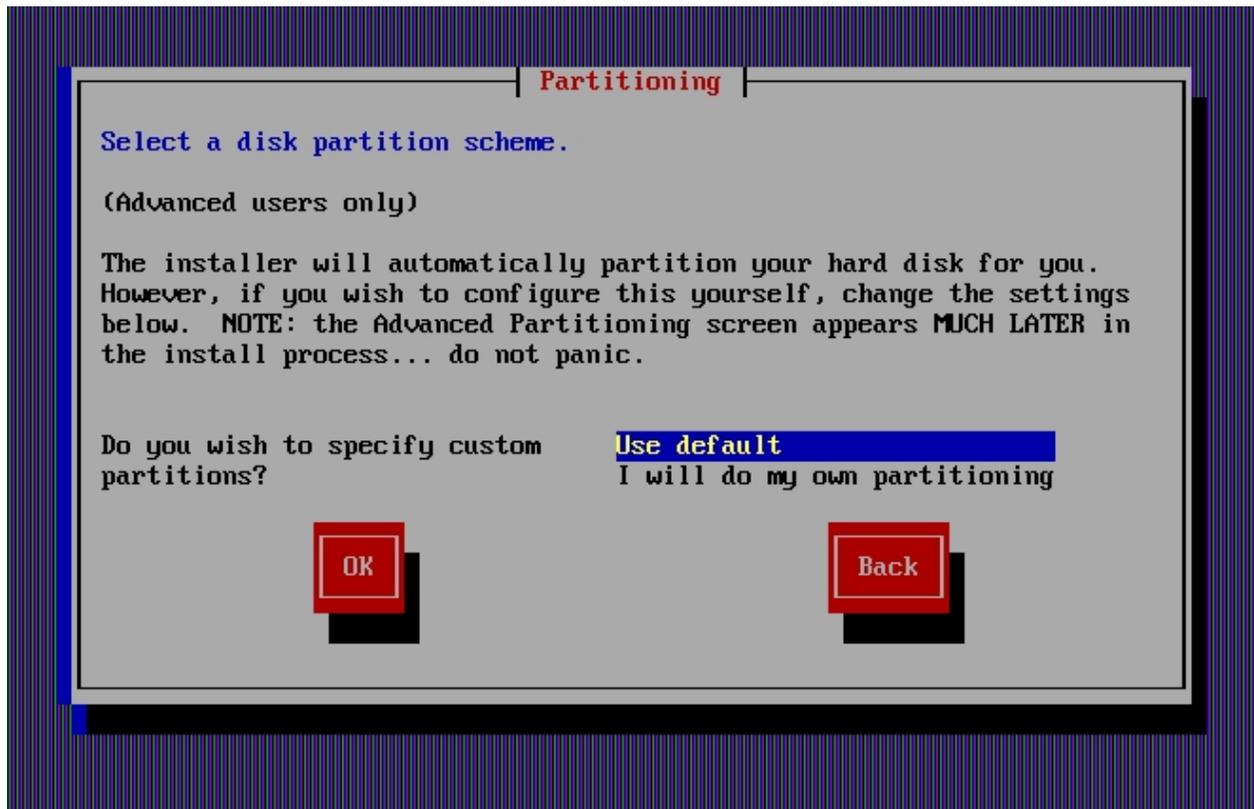
arriba y obtener algo así:

```
-->esta-es-mi-contraseña  
--> eSTAEsmIcONTRASENA  
--> 3$T43$m1cONTR4$3N4
```

[Imagen 27]



[Imagen 28]



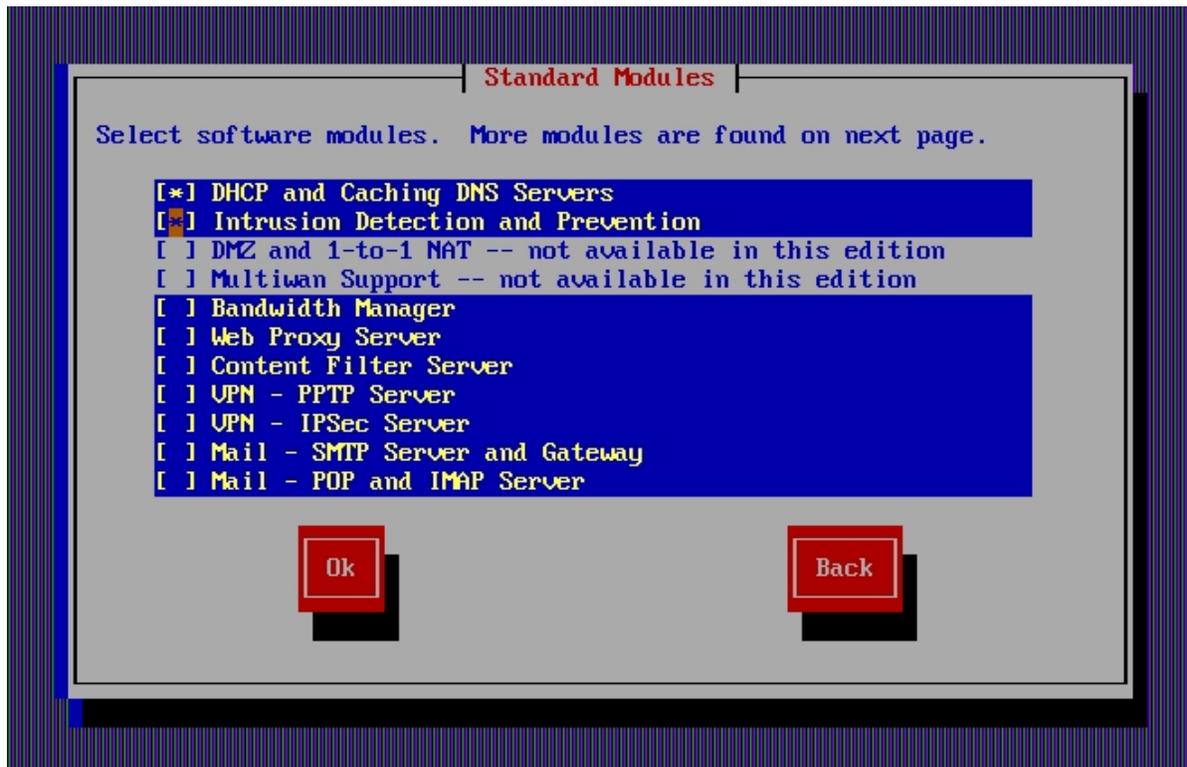
Llegamos ahora a la sección mas critica de la instalación, si hacemos algo mal aquí, podemos hacer muchos daños. “Particionar” un disco es dividir en varias secciones este mismo, es una forma barata y práctica de tener varios discos duros en un computador, por así decirlo. Esto es importante en un sistema de archivos *Linux* ya que en las diferentes particiones principales irán las diferentes jerarquías, archivos y datos. El esquema principal de un sistema *Linux* en *ClarkConnect* se conforma de tres particiones: la raíz /, la /var y la swap. (Mirar tabla de 'Ejemplo de la jerarquía del sistema de archivos en *Linux*').

Este esquema se construye cuando se escoge el “particionado” predefinido. En cambio si se quiere realizar un “particionado” diferente para modificar el tamaño, el tipo y el formato de las particiones, también es posible. Explicar cómo realizar este proceso para partir el disco no es fácil y no menos extenso, por ello, explicaré mas adelante cómo hacerlo. En general, las particiones por defecto son suficientes para la mayoría de los usuarios, así que no habrá problemas si seleccionamos esta opción. Para instalar todo el sistema operativo con los módulos necesarios, un disco duro con un mínimo de 4 GB de espacio es suficiente\*; pero si se desea guardar mas archivos de *log* e información sobre los usuarios y actividades del servidor es mejor un disco duro de 20 GB como mínimo. El sistema operativo base y los módulos ocupan cerca de 2 GB, el espacio restante es para la *Swap* y la partición */var* donde se guardan los *logs*.

---

\* Este valor es, en la opinión del autor, lo mínimo requerido para que el servidor funcione correctamente. Originalmente la documentación oficial recomienda 1 GB de espacio.

[Imagen 29]



Continuando con la instalación llegamos a la sección donde escogemos los módulos<sup>29</sup> a instalar. Los módulos que no seleccionemos aquí podrán instalarse posteriormente a través de la interfaz Web o por línea de comando.

A continuación explicaré brevemente cada módulo:

---

<sup>29</sup> Sección de *software* que puede ser fácilmente removida o instalada en un sistema sin afectar la integridad de este. Los módulos de *software* permiten añadir nuevas posibilidad y opciones al Servidor/*Firewall*.

**-DHCP<sup>30</sup> and Caching DNS Servers:** servidor *DHCP* para proveer a clientes en una red de direcciones *IP* asignadas en un rango por el administrador de la red, esto elimina la necesidad de configurar manualmente cada nuevo cliente en la red.

**-Intrusion Detection and Prevention:** como su nombre lo dice, módulo para detectar y prevenir intrusos en la red. El *software* es capaz de detectar y reportar tráfico inusual en la red incluyendo intentos de *hacking*, *Malware* y escaneo de puertos. El otro *software*, bloquea a supuestos atacantes del sistema, posee una base de datos actualizada con más de 2000 reglas.

**-Bandwidth Manager:** el módulo controla el ancho de banda que pasa a través del Servidor/Firewall. Este módulo se usa para darle prioridad a un tráfico especial entrante y saliente de la red, como por ejemplo: las llamadas por voz-IP.

Adicionalmente, se puede limitar el uso del ancho de banda para determinados rangos de *IP* en la red, puertos y rangos de puertos.

**-Web Proxy Server:** servidor *Proxy*<sup>31</sup> y de caché, con la habilidad de ayudar en el manejo de ancho de banda y ayuda a registrar la actividad de los usuarios.

**-Content Filter Server:** módulo para filtrar el contenido Web, funciona bloqueando las páginas Web inapropiadas para el usuario final, el *software* puede bloquear también páginas como *Hotmail* para aumentar así la productividad de los usuarios. Para bloquear el contenido utiliza una variedad de métodos como comparación de frases, filtrado de *URL*<sup>32</sup>,

---

30 *Dynamic Host Configuration Protocol*, permite la configuración automática del protocolo *TCP/IP* de todos los clientes en la red.

31 *Software* que permite a varios clientes conectarse a Internet a través de una única conexión física a Internet.

32 *Uniform Resource Locator*, Localizador Unificado de Recursos. Dirección a través de

entre otros.

**-VPN<sup>33</sup> - PPTP Server:** servidor VPN privado para conectarse remotamente a escritorios *Windows*® de forma segura.

**-VPN - IPSec Server:** servidor VPN privado para conectar una LAN con otra LAN a través de la interfaz Web.

**-Mail - SMTP<sup>34</sup> Server and Gateway:** módulo para administrar un servidor de correo electrónico propio. Posee control de SPAM y de virus.

**-Mail - POP<sup>35</sup> and IMAP<sup>36</sup> Server:** este módulo da la posibilidad para que los clientes descarguen sus correos electrónicos por POP o IMAP a sus máquinas.

**-Mail - Antivirus Server:** el *software* escanea los correos electrónicos que pasan por el servidor en busca de virus y otras amenazas.

**-Mail - Antispam Server:** el *software antispam* funciona en conjunto con el servidor de correo, este identifica el SPAM usando diferentes algoritmos, además *ClarkConnect* incluye listas grises y negras adicionales, las cuales son muy útiles para detectar SPAM.

**-Webmail:** *software* que permite a usuarios sin cliente de correo revisar su correo desde cualquier computador conectado a Internet.

**-Flexshare File Manager:** es un módulo flexible y seguro diseñado como una herramienta de colaboración que integra cuatro de los métodos más comunes para comunicarse e intercambiar archivos: Web

---

la cual se accede a las páginas Web en Internet o a otros ordenadores en la red.

33 *Virtual Private Network*, Red Privada Virtual. Conexión entre dos o más sistemas a través de una red pública, como Internet, para intercambiar información de forma segura y cifrada.

34 *Simple Mail Transfer Protocol*, protocolo de transferencia simple de correo, por el cual se envía (exclusivamente) correo electrónico en Internet.

35 *Post Office Protocol*, Protocolo de oficina de correos. Estándar de correo electrónico, usa un buzón para acumular los mensajes de un usuario.

36 *Internet Message Access Protocol*. Protocolo por el cual se accede a mensajes (correos) electrónicos almacenados en un servidor.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

(HTTP<sup>37</sup>/HTTPS)<sup>38</sup>, FTP (FTP/FTPS)<sup>39</sup>, File Shares (Samba<sup>40</sup>) e E-mail (SMTP/MIME/SMIME).

-**Web Server**: servidor Web Apache para publicar páginas Web.

-**FTP Server**: servidor FTP para compartir archivos de forma sencilla.

-**File Server (Samba)**: Sistema para compartir archivos y otros recursos entre Windows® y Linux. Ejemplo: en el servidor, en una carpeta, los usuarios guardan archivos para compartir, accesibles desde un explorador desde un ambiente Windows®. También se pueden compartir impresoras.

-**File Server Antivirus**: módulo que escanea los archivos en el servidor en busca de virus.

-**Backup for Server and LAN**: software capaz de crear, administrar y recobrar copias de seguridad en los computadores de una LAN en una variedad de SO. Tiene soporte para diversos dispositivos de almacenamiento.

-**Print Server**: módulo para el servidor de impresoras, para que los usuarios puedan imprimir a través de la red.

-**Database Server**: software de base de datos MySQL<sup>41</sup> “administrable” desde una interfaz Web.

---

37 *Hyper Text Transfer Protocol*, protocolo de transferencia de hipertexto. Se usa como sistema de comunicación y transferencia para visualizar páginas Web desde un navegador.

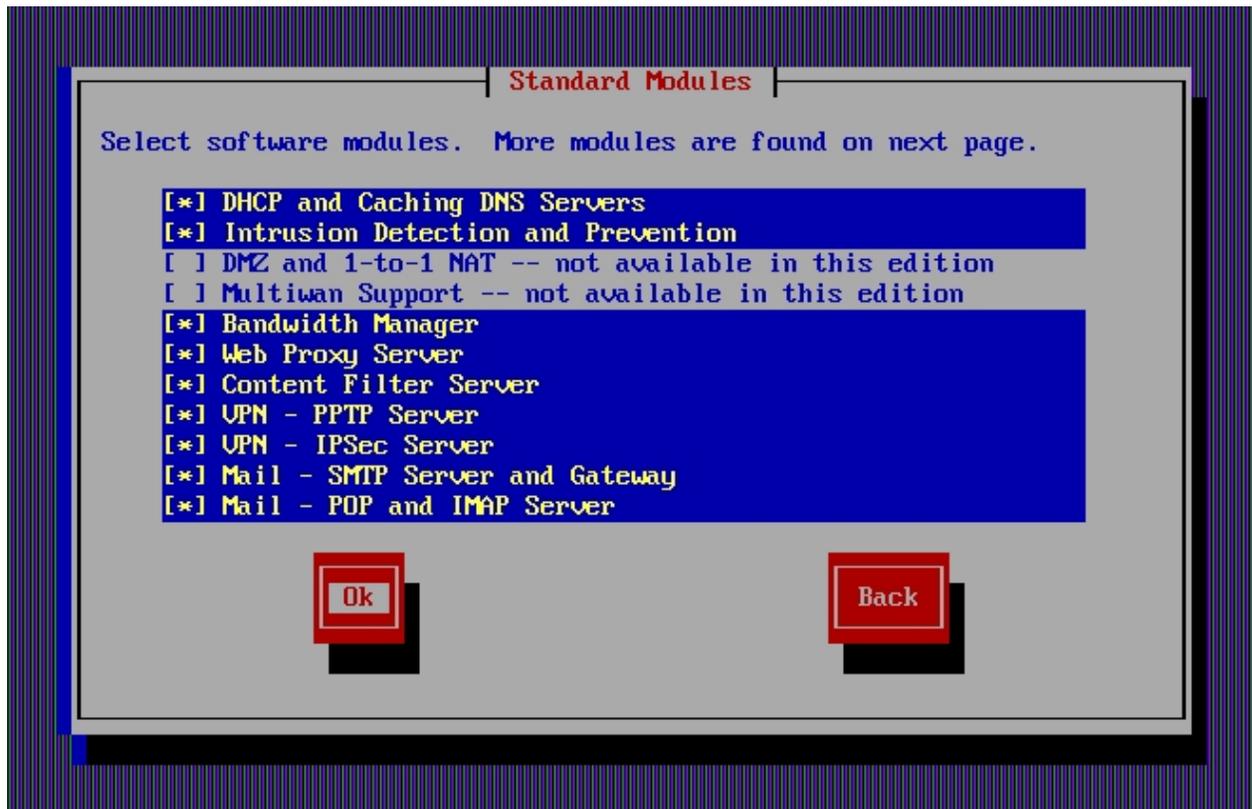
38 *Secure Hyper Text Transfer Protocol*, protocolo de transferencia segura de hipertexto, se usa para realizar conexiones HTTP para transferencia de contenido, pero de forma segura.

39 *File Transfer Protocol*, se usa para transferir archivos de un sistema a otro.

40 Es un software que permite compartir archivos e impresoras con otros computadores en la misma red.

41 Sistema de gestión de bases de datos de código abierto.

[Imagen 30]



Para el Servidor/*Firewall* necesitaremos los módulos de DHCP, Bandwidth Manager, Web Proxy Server y Content Filter Server; si se desea tener protección para la detección y prevención de ataques informáticos en la red del servidor, es necesario instalar el segundo módulo. Para seleccionar nos movemos con los cursores y presionamos la barra espaciadora.

Este *software* seleccionado es el necesario para ejecutar la tarea de Servidor/*Firewall* en el entorno escolar; si se desean otras posibilidades para realizar con el servidor, como por ejemplo compartir archivos, sólo basta con seleccionar el módulo

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

correspondiente. Los módulos restantes pueden seleccionarse de igual forma para instalarse; estos no afectan el Servidor/Firewall en su funcionamiento a excepción de hacerlo más lento durante el arranque y apagado del sistema. Continuamos presionando *Enter* sobre *oK* y llegamos a otra pantalla con más módulos a instalar. Realizamos el mismo proceso anterior.

[Imagen 31]



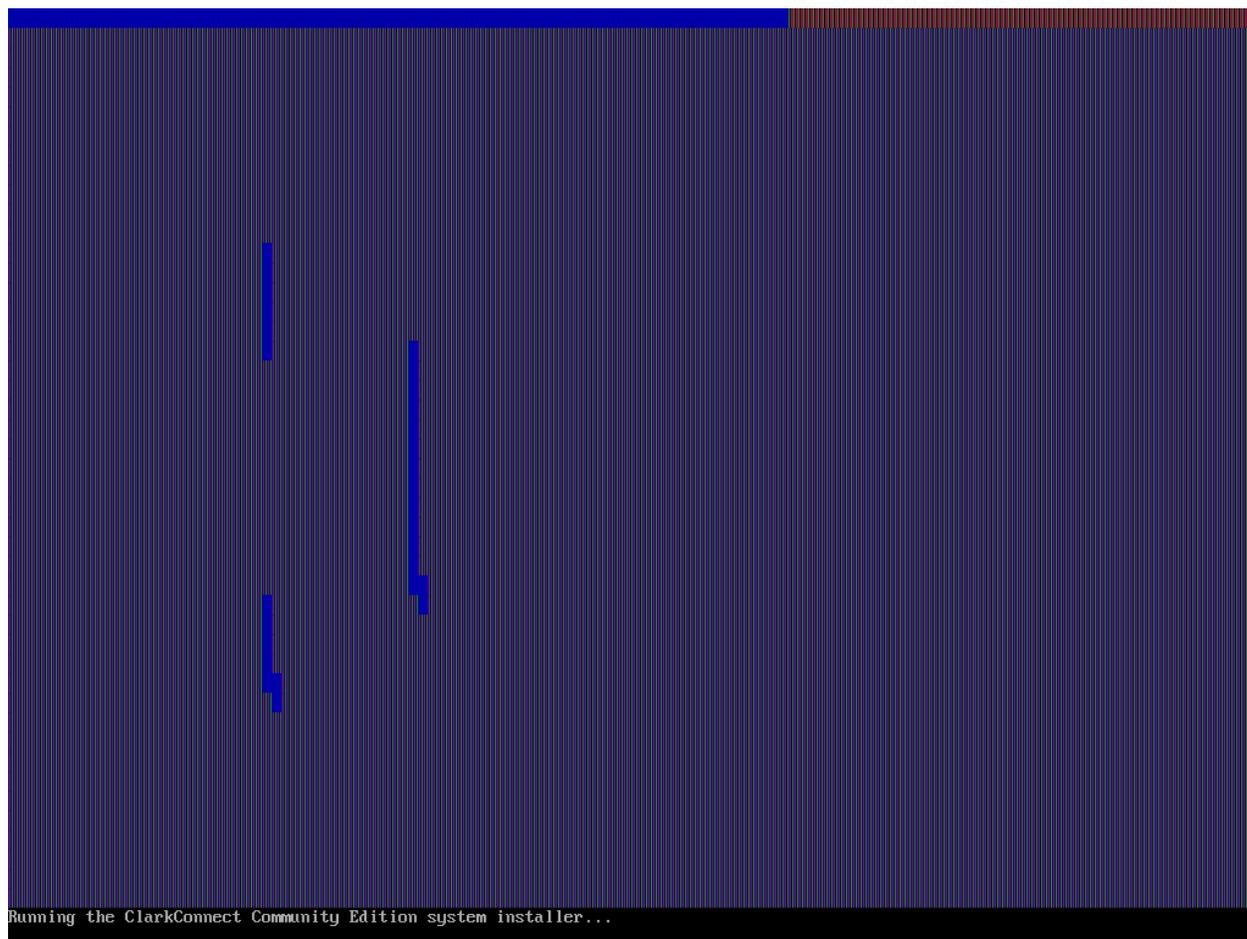
[Imagen 32]



¡Felicitaciones! Acabamos de finalizar la etapa de configuración para la instalación. Ahora aparece una advertencia y suponiendo que estamos seguros en lo que vamos a hacer presionamos Done.

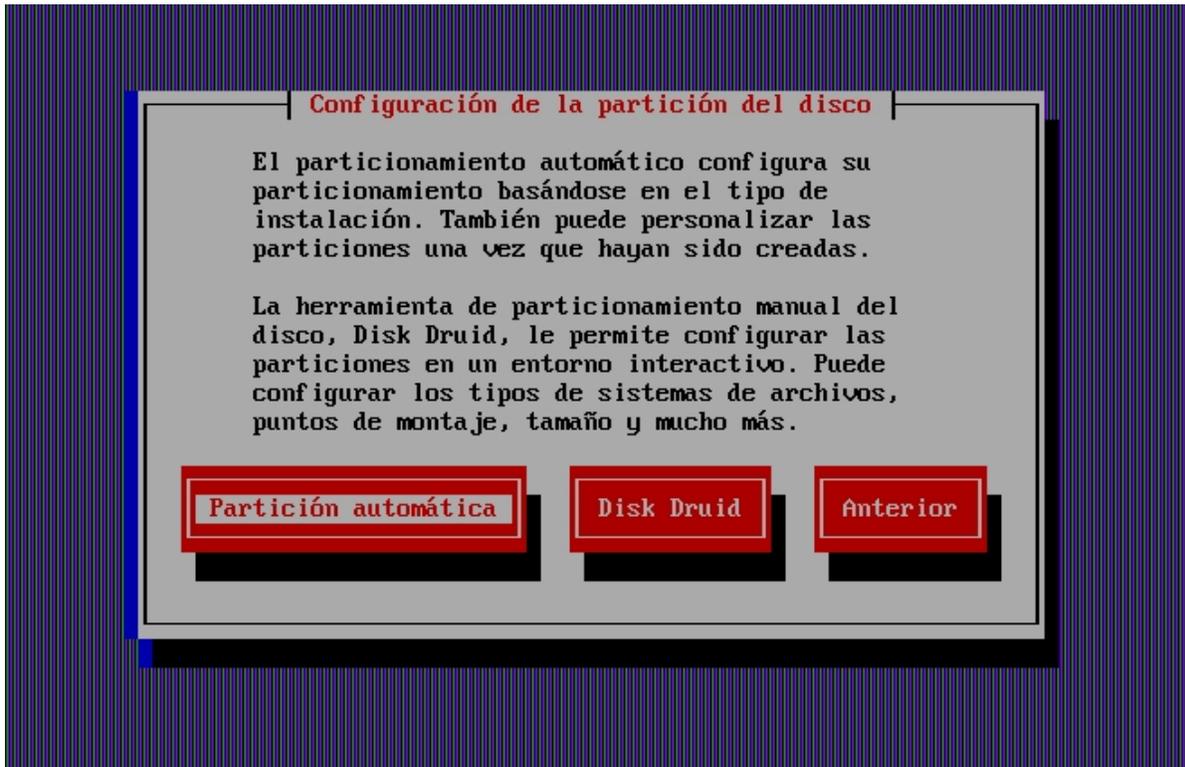
Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 33]



En esta etapa comienza a correr el instalador del *ClarkConnect*.

[Imagen 34]



Si seleccionamos antes realizar el “particionado” manual, aparecerá una pantalla donde nos preguntará cómo “particionar” el disco (¡mirar la sección siguiente!).

De lo contrario, comenzará con la instalación sin preguntar nada más. Después de unos segundos nos muestra qué operaciones realiza.

Recomiendo esta opción, ya que “particionar” un disco duro puede ser riesgoso y debe realizarse sólo por usuarios con los conocimientos específicos. Además, el “particionado” automático nos ahorra tiempo.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 47]



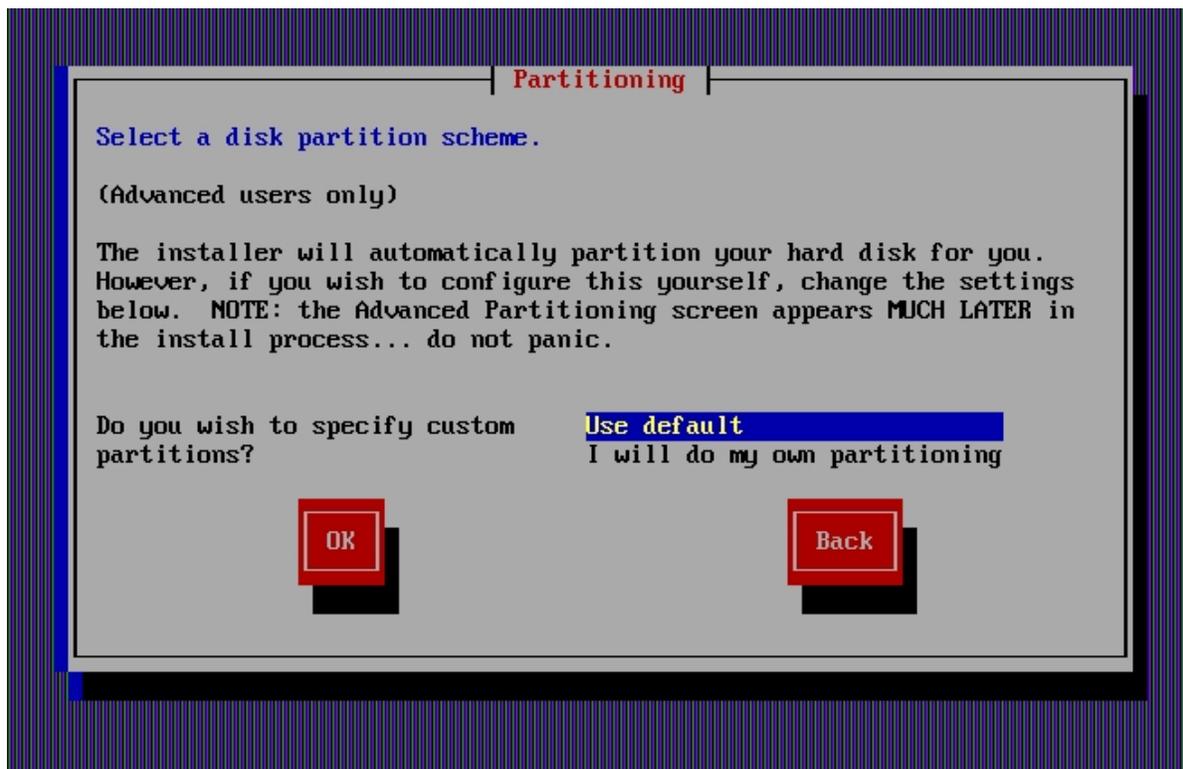
## **4.5.2 “PARTICIONANDO” MANUALMENTE EL DISCO DURO Y CONFIGURACIÓN DEL GESTOR DE ARRANQUE**

En esta sección hablaré y mostraré cómo “particionar” el disco duro manualmente.

**¡ADVERTENCIA!** ¡Lo que aparece a continuación no se recomienda para usuarios novatos, nadie es responsable por lo que suceda a continuación con su disco duro, a excepción de usted!

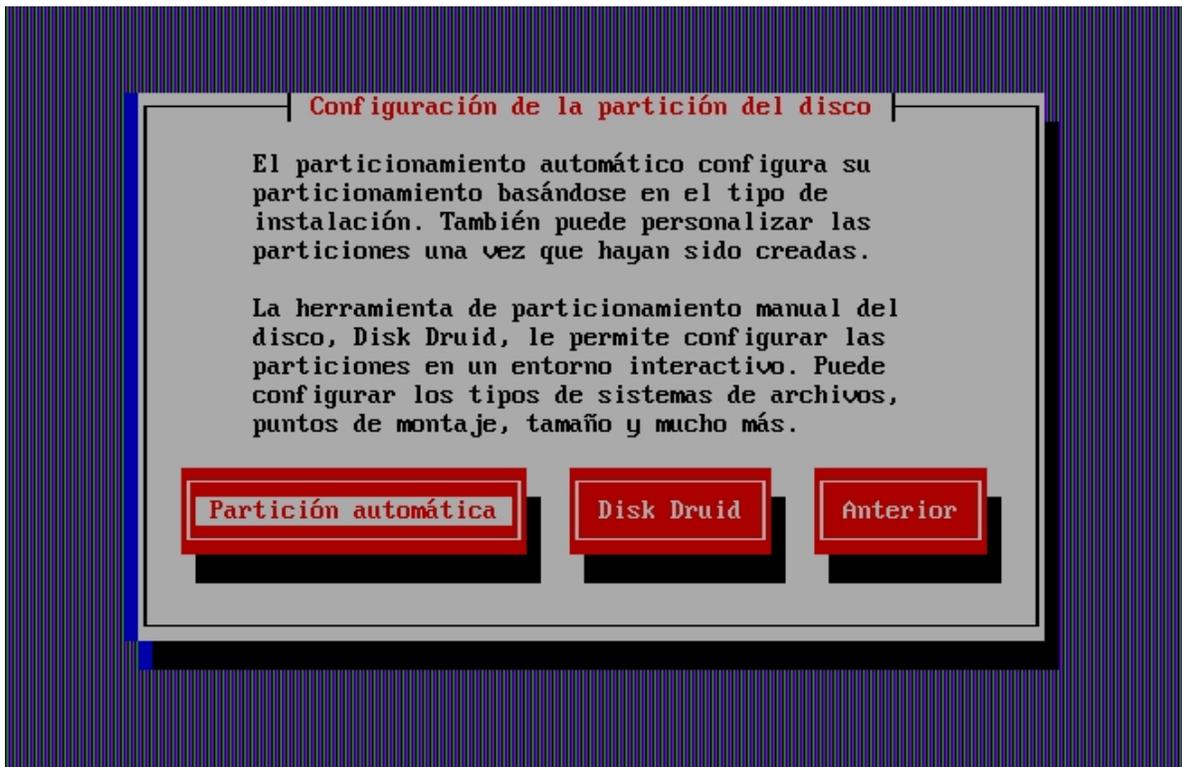
Ahora bien, después de la pantalla, cuando preguntaban la contraseña para el servidor, continuaba la del “particionado” y allí se decidía si realizar el “particionado” manual o el por defecto. Si estás aquí, es porque elegiste el manual, ¿no?

[Imagen 28]



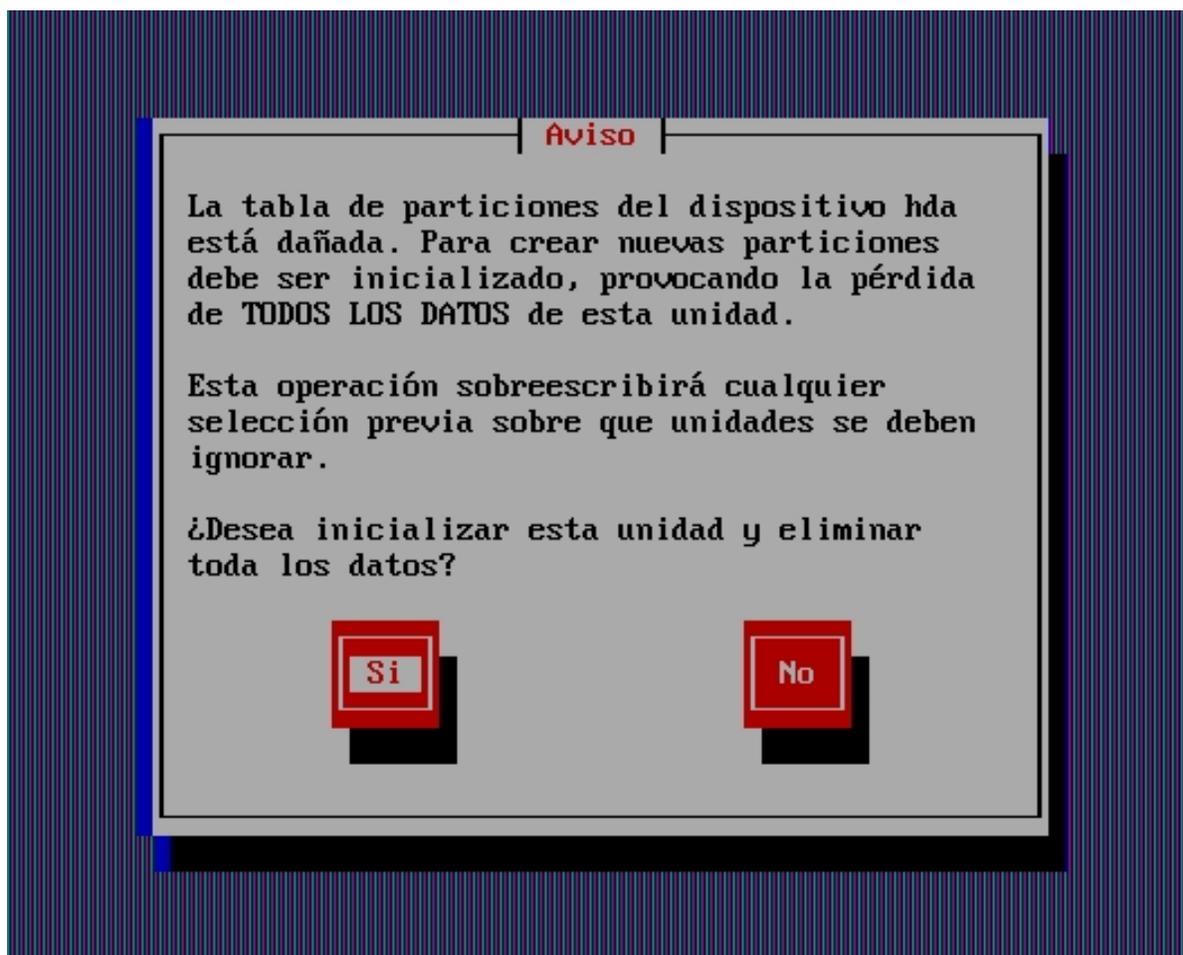
Bien, después de terminar de configurar la instalación nos preguntan en la sección 'Configuración de la partición de disco', qué opción queremos llevar a cabo. Allí presionaremos sobre Disk Druid que nos ayudará a partir el disco como lo queremos.

[Imagen 34]



Si aparece un aviso sobre la tabla de particiones dañada, hacer caso omiso y presionar sí.

[Imagen 35]



Llegamos a una ventana que nos muestra el dispositivo `/dev/hda`<sup>42</sup> (así se llama mi disco duro, pero pueden existir otras denominaciones como `/dev/sda`) y su espacio libre; ese es el disco duro. Si existen otros discos duros en el servidor, aquí mismo aparecerán.

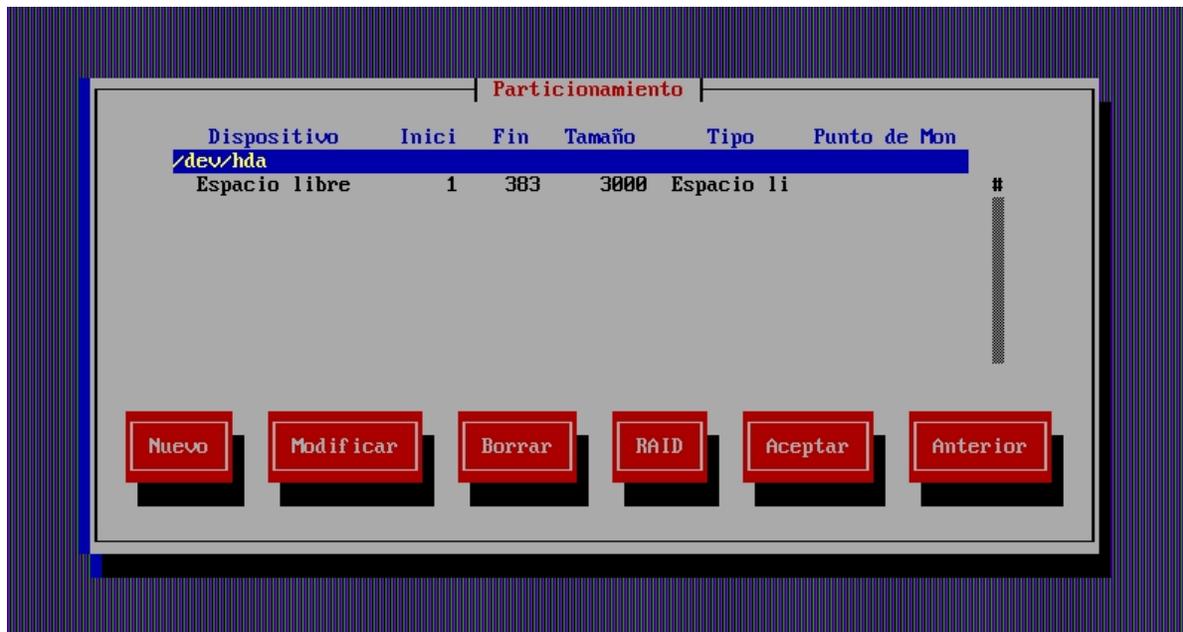
Seleccionamos `Free Space` y presionamos `New` o la tecla `F2`. Aquí

---

<sup>42</sup> Enlaces que apuntan al hardware de la máquina.

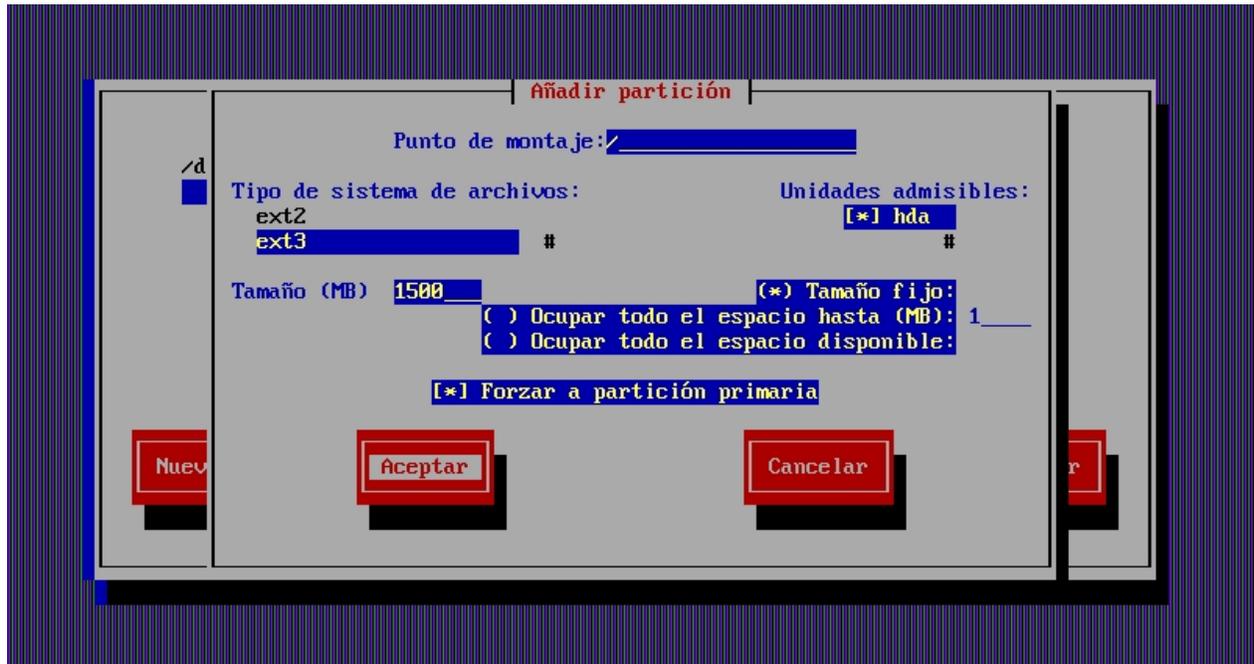
nos permite añadir la siguiente partición.

[Imagen 36]



En la imagen se puede visualizar que he modificado las opciones, para hacer esto nos movemos con `Tab` y los cursores. Lo primero que realizaremos es la partición raíz o `/`, esta es la raíz del sistema de archivos de *Linux*.

[Imagen 37]



En punto de montaje escribimos dónde se colgará la partición en el sistema de archivos. Seleccionamos Tipo de sistema de archivos `ext3`<sup>43</sup>, el cual es sistema de archivos mas usado para *Linux* porque brinda estabilidad, seguridad y velocidad. Pasamos al tamaño, este se debe especificar en *MegaBytes (MB)*, *1024 MB* equivalen a un *1 GigaByte*. Para la partición raíz `/` se necesitan mínimo *2 GB*, pero recomiendo un tamaño entre *5 y 10 GB*. Las otras opciones no son de mucha importancia a excepción de la última para nuestro caso. Presionamos `Aceptar` y terminamos de definir la primera partición.

<sup>43</sup> *EXT3 (third extended filesystem* o tercer sistema de archivos extendido) es un sistema de archivos, el cual es usado ampliamente por las distribuciones de *Linux*.

**¡ATENCIÓN! ¡Si se desea realizar una partición /boot para hospedar el gestor de arranque, esta debe ser preferiblemente la primera partición para así evitar futuras confusiones! Esta partición no necesita más de 120 MB de espacio libre y debe ser primaria.**

**Tabla 7 - Ejemplo de la jerarquía (estructura) del sistema de archivos en Linux**

<b>/</b>	La raíz, de aquí cuelgan las carpetas principales
<b>/bin</b>	Contiene los archivos ejecutables principales y fundamentales del SO
<b>/boot</b>	Contiene al gestor de arranque
<b>/dev</b>	Alberga los puntos de entrada para los periféricos
<b>/etc</b>	Contiene los comandos y archivos que el Superusuario ( <i>root</i> ) más necesita
<b>/home</b>	Carpeta donde se encuentran los directorios de cada usuario
<b>/lib</b>	Archivos, librerías y directorios fundamentales para el inicio del sistema
<b>/mnt</b>	Punto de montaje de las particiones temporales ( <i>CD-ROM</i> , disquete, <i>USB-DISK</i> )
<b>/opt</b>	Almacena los paquetes de las aplicaciones suplementarias
<b>/proc</b>	Pseudo sistema de archivos que funciona como interfaz para el <i>kernel</i>
<b>/root</b>	Carpeta del Superusuario
<b>/sbin</b>	Contiene binarios fundamentales
<b>/tmp</b>	Aquí se guardan los archivos temporales
<b>/usr</b>	Alberga toda una jerarquía secundaria con los archivos y carpetas más usados por los usuarios
<b>/var</b>	Contiene datos variables, como por ejemplo <i>logs</i> del sistema

Ahora continuamos con la segunda partición /var. De igual forma que la anterior, se define esta partición; lo único que cambia es el tamaño. Se recomienda que sea de entre 35% y 50% del espacio total disponible.

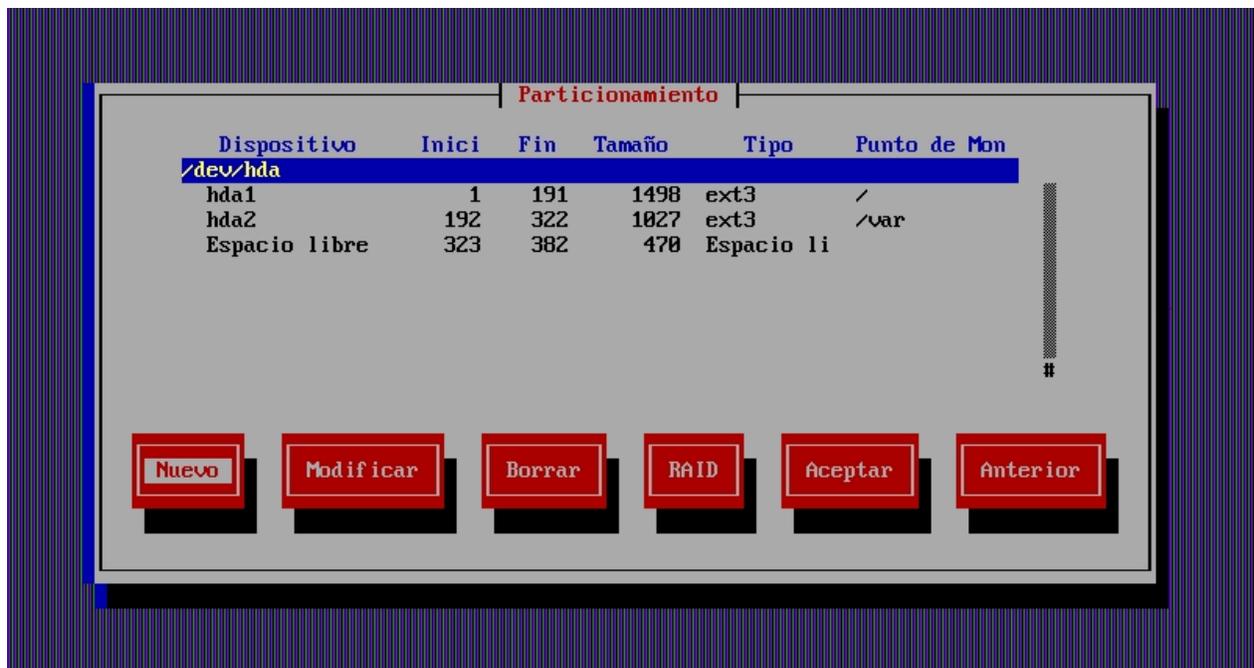
[Imagen 38]



Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

Volvemos a la tabla de particiones y observamos que aún tenemos un espacio libre. Éste será para la *Swap*, que es la memoria de intercambio. Aquí se guardan los datos y los programas que el *kernel* no necesita por el momento para así ahorrar espacio en la memoria RAM que es más rápida a comparación de la *Swap*. ¡Esta memoria de intercambio debe tener el doble de la memoria RAM disponible pero con un máximo de 2 GB!

[Imagen 39]

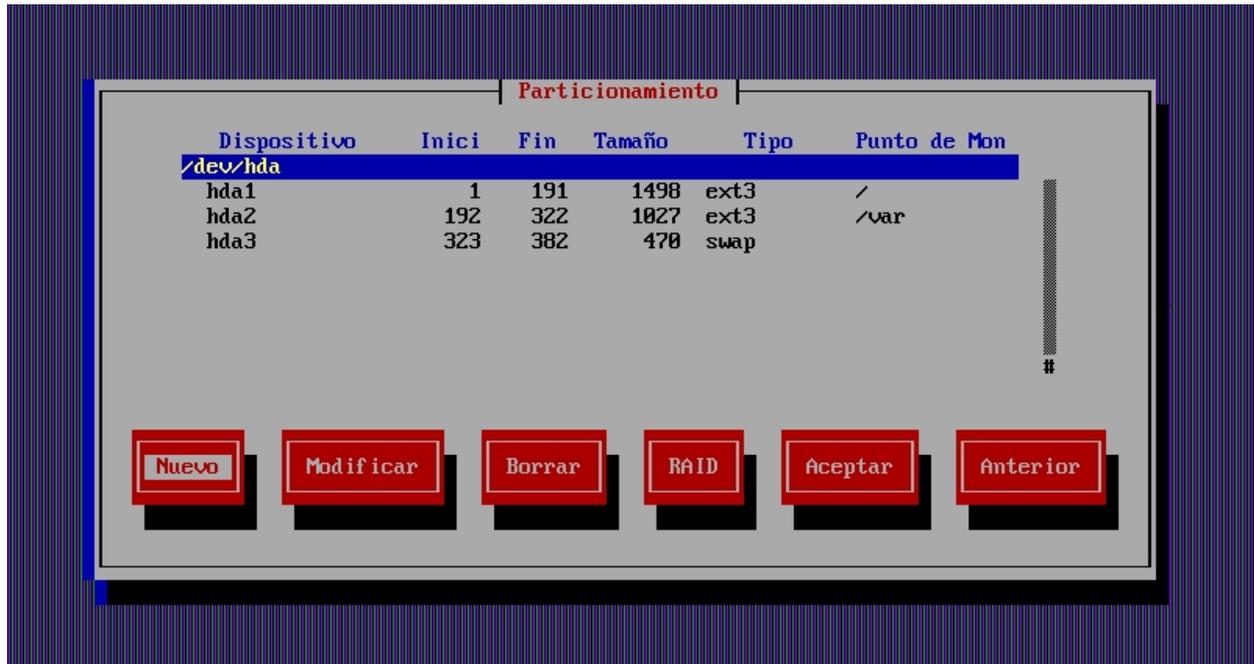


Seleccionamos el espacio libre disponible y presionamos **Nuevo**. Esta vez no escribiremos ningún punto de montaje, en vez de eso bajaremos al tipo de sistema de archivos y buscamos **swap**. E igualmente como las anteriores le definimos el espacio que ocupará en el disco duro.

[Imagen 40]



[Imagen 41]



Este tipo de “particionado” es el común para este servidor pero no es obligatorio.

Si sabemos que muchos usuarios compartirán archivos y datos, es mejor definir la partición `/home`, adicionalmente a las anteriores; esta debe tener por lo menos 10 GB de espacio libre.

Visualizamos por última vez la tabla de particiones para buscar posibles errores o problemas en el tamaño o jerarquía. Si nos encontramos conformes con ésta, presionamos `Aceptar`.

A continuación nos pregunta el instalador si queremos instalar un gestor de arranque que por defecto es *GRUB*. Lo seleccionamos y continuamos.

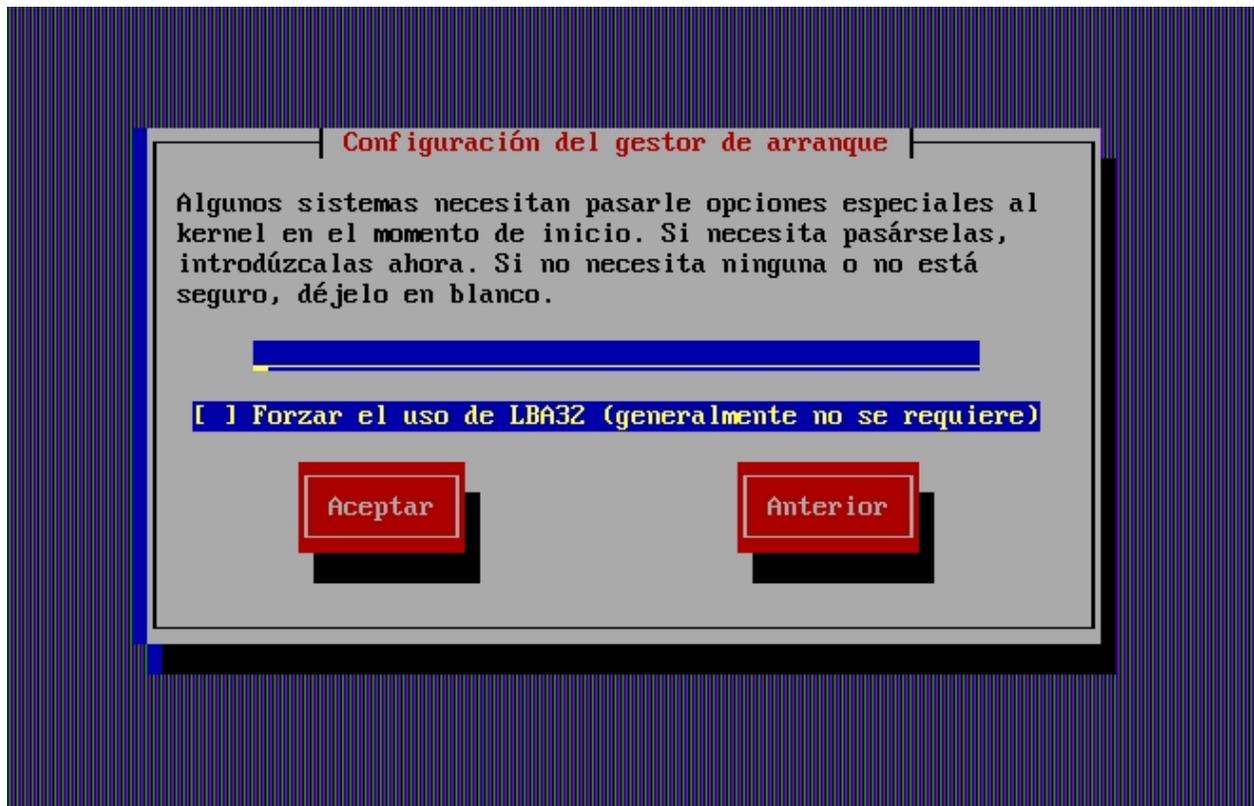
[Imagen 42]



Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

Esta sección para la configuración del gestor de arranque no se usa comúnmente ya que los servidores donde se ejecuta el *ClarkConnect* son compatibles con *Linux*. Así que le hacemos caso omiso y seguimos adelante.

[Imagen 43]



**¡¡IMPORTANTE!** Una contraseña para el GRUB evita que usuarios sin autorización ingresen al servidor físicamente y modifiquen algo. Un usuario avanzado sabe que si escribe `single` al final de la línea que inicia el *kernel*, éste no pedirá la contraseña de *root* para ingresar al SO y le permitirá modificar ésta sin problemas. Una falla de seguridad que es mejor evitar.

[Imagen 44]



Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

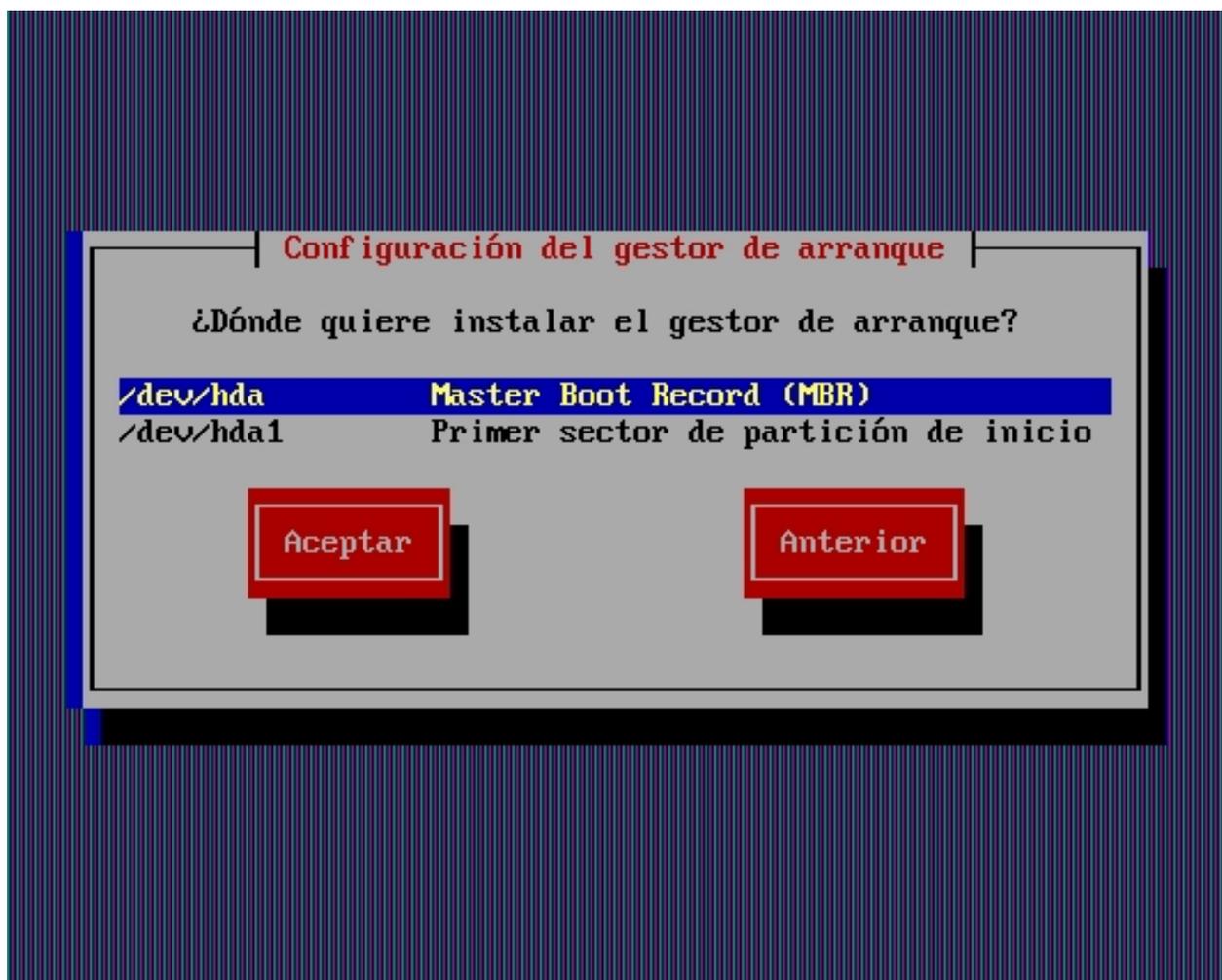
Si poseemos un solo SO en la máquina no nos tenemos que preocupar en esta sección, sigamos con Aceptar.

[Imagen 45]



A continuación tenemos que seleccionar en que partición queremos instalar el *GRUB*. Si no creamos una partición */boot*, seleccionamos */dev/hda* (siendo *hda* el disco duro donde se encuentra el *ClarkConnect*), de lo contrario escogemos la partición que creamos para el */boot*.

[Imagen 46]



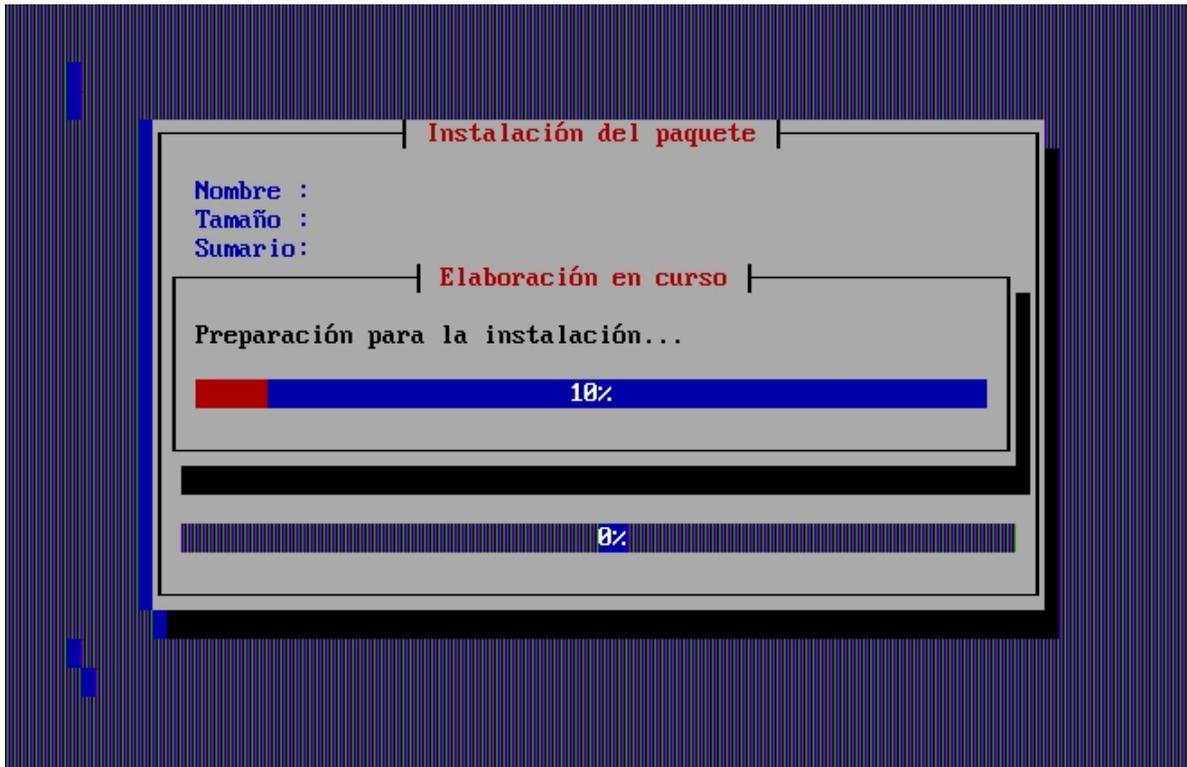
Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

¡Hemos finalizado con la configuración para el instalador! Sólo basta esperar mientras se instala y carga todos los archivos necesarios para el Servidor/Firewall.

[Imagen 47]

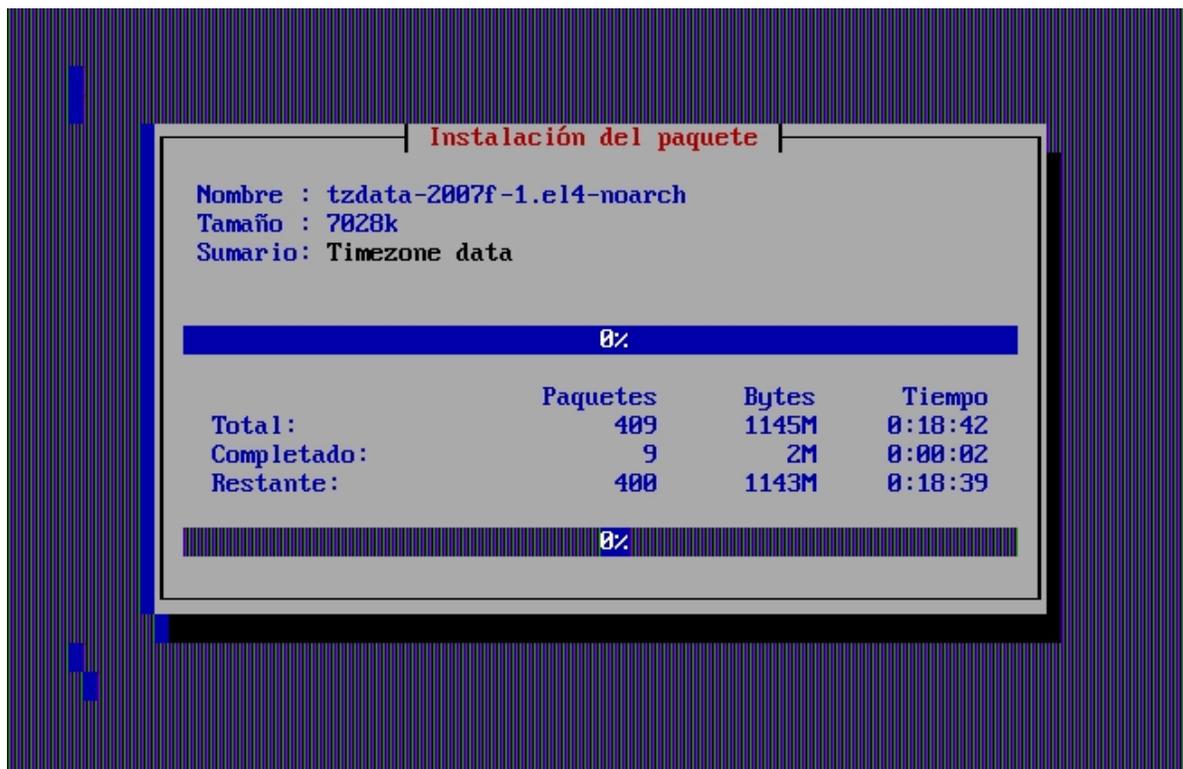


[Imagen 48]

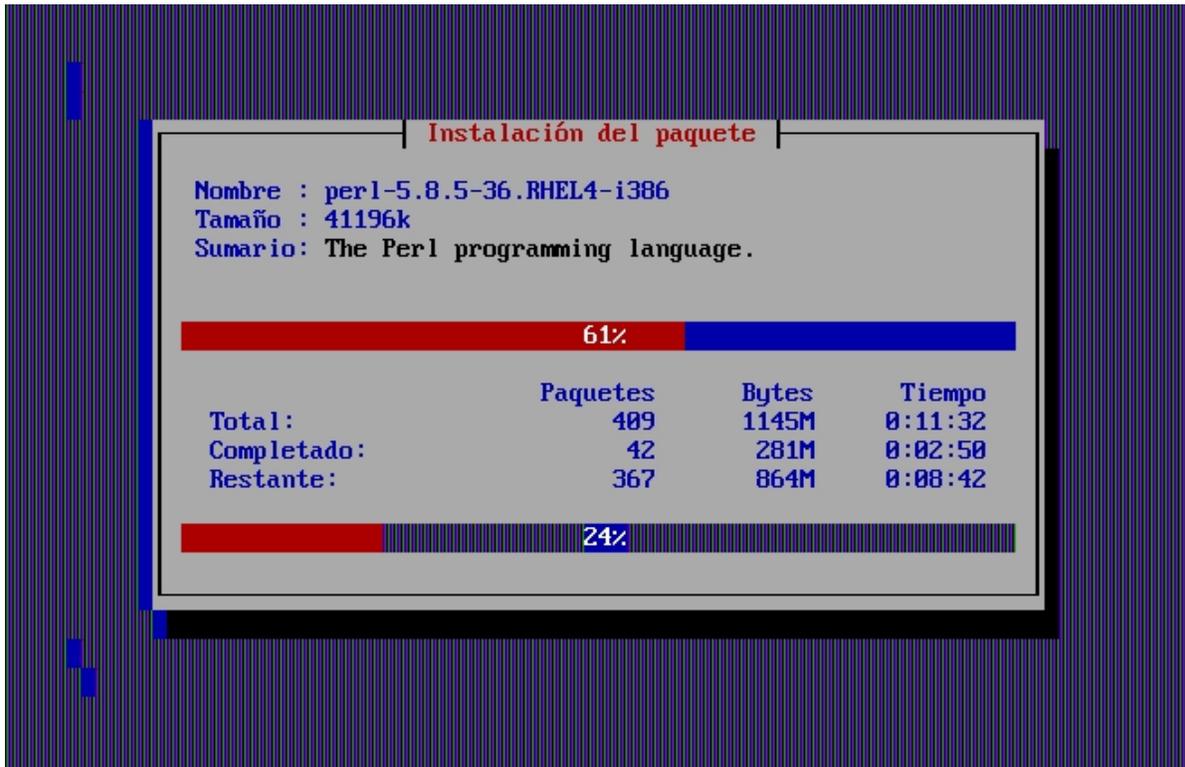


Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 49]

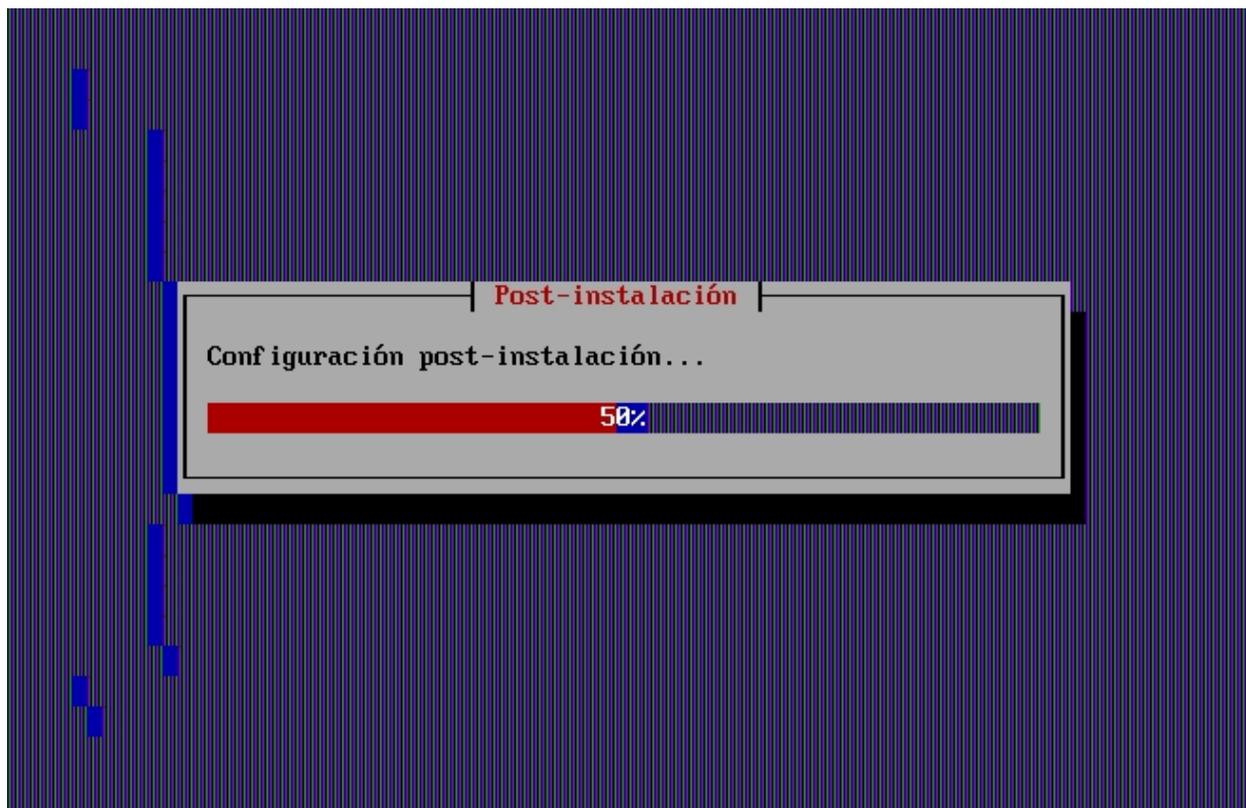


[Imagen 50]



Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 51]



Minutos después de comenzar con la instalación, nos muestra un último mensaje. Ahora que la instalación está completa procedemos a retirar el *CD-ROM* y a reiniciar el computador (presionando *Enter*).

[Imagen 52]

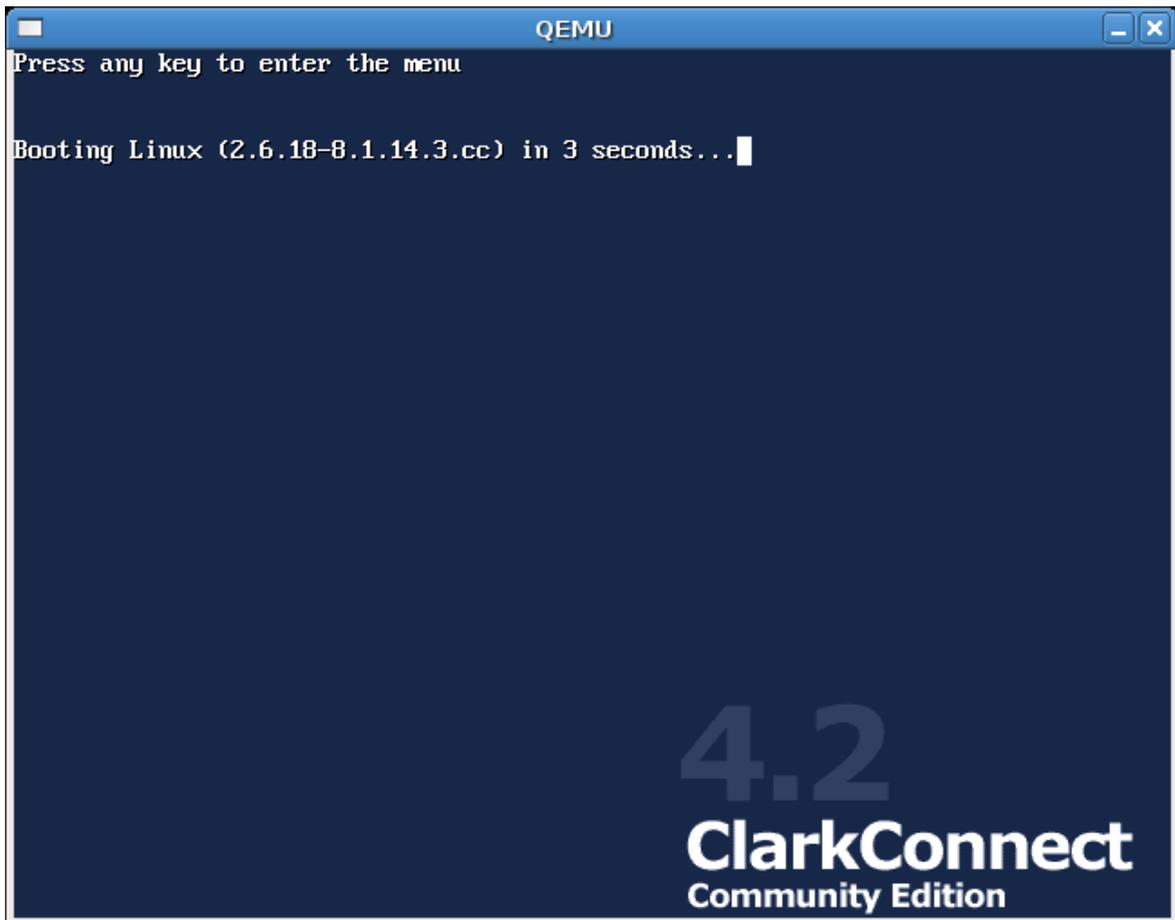


## **CAPITULO 5**

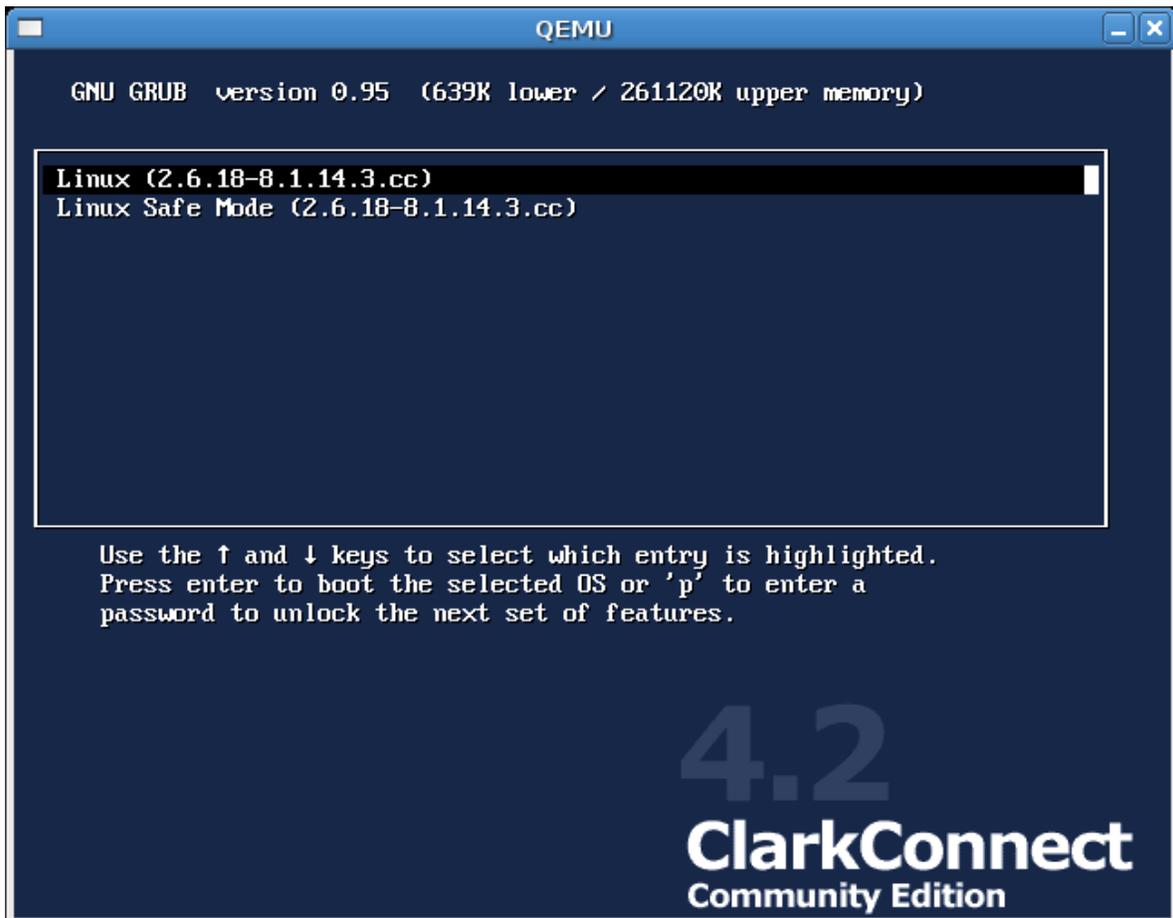
### **5.1 POST-INSTALACIÓN**

Acabamos de instalar el *ClarkConnect* 4.2 en el sistema y hemos reiniciado, en la primera fase del inicio observamos una pantalla, el *GRUB*, si presionamos cualquier tecla vemos las dos opciones que podemos usar para arrancar el *Linux*. Si se especificó una contraseña para el *GRUB* durante la instalación cualquier modificación que se desee realizar en esta fase requerirá autenticación.

[Imagen 53]



[Imagen 54]



Continuando con el inicio del sistema a continuación se muestra en pantalla como el servidor inicia los servicios y programas para su funcionamiento. Si se le pone atención a las líneas de texto se pueden encontrar datos útiles, como por ejemplo: en qué estado se encuentra el *hardware* y si la red ha subido correctamente.

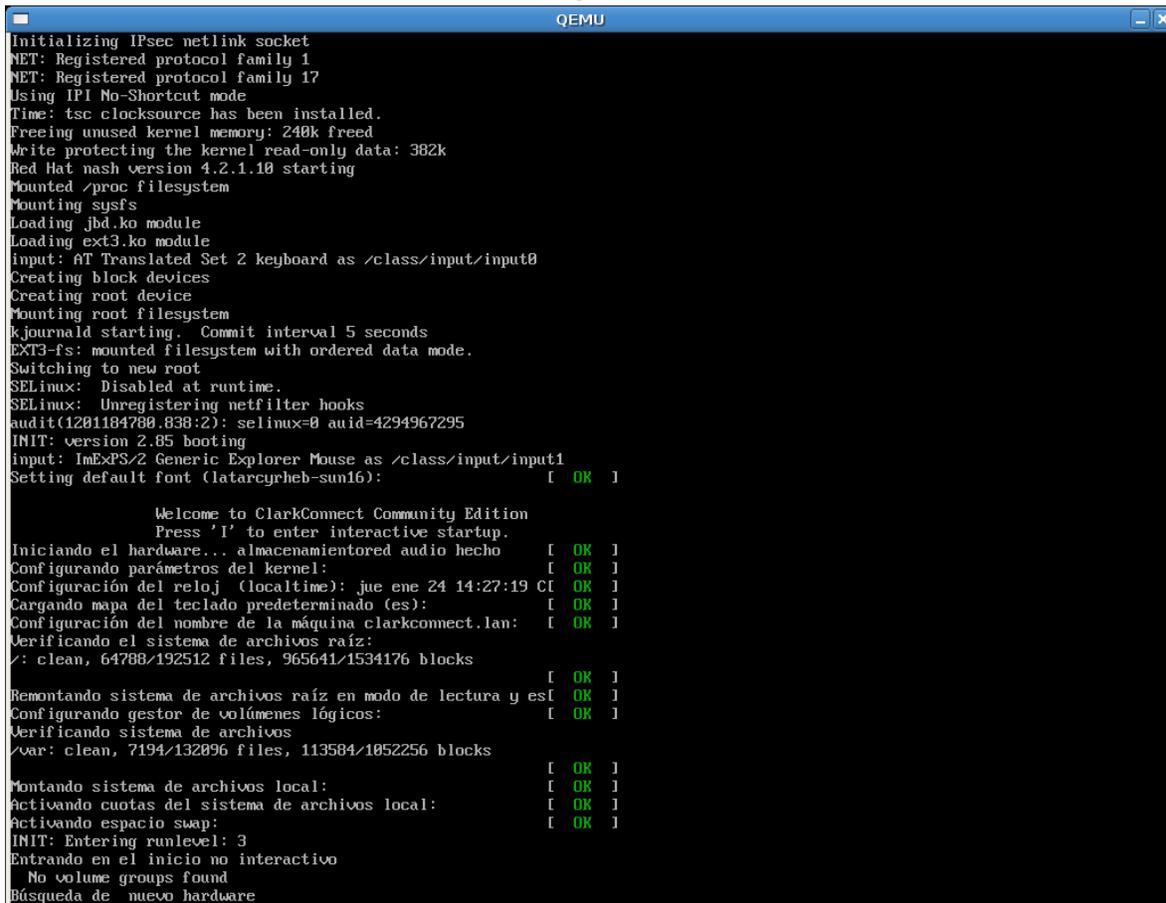
[Imagen 55]

```
QEMU
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
hdc: QEMU CD-ROM, ATAPI CD/DVD-ROM drive
ide1 at 0x170-0x177,0x376 on irq 15
hda: max request size: 512KiB
hda: 6144000 sectors (3145 MB) w/256KiB Cache, CHS=6095/255/63, (U)DMA
hda: cache flushes supported
   hda: hda1 hda2 hda3
ide-floppy driver 0.99.newide
usbcore: registered new driver hiddev
usbcore: registered new driver usbhid
drivers/usb/input/hid-core.c: v2.6:USB HID core driver
PNP: No PS/2 controller found. Probing ports directly.
serio: i8042 AUX port at 0x60,0x64 irq 12
serio: i8042 KBD port at 0x60,0x64 irq 1
mice: PS/2 mouse device common for all mice
md: md driver 0.90.3 MAX_MD_DEVS=256, MD_SB_DISKS=27
md: bitmap version 4.39
TCP bic registered
Initializing IPsec netlink socket
NET: Registered protocol family 1
NET: Registered protocol family 17
Using IPI No-Shortcut mode
Time: tsc clocksource has been installed.
Freeing unused kernel memory: 240k freed
Write protecting the kernel read-only data: 382k
Red Hat nash version 4.2.1.10 starting
Mounted /proc filesystem
Mounting sysfs
Loading jbd.ko module
Loading ext3.ko module
input: AT Translated Set 2 keyboard as /class/input/input0
Creating block devices
Creating root device
Mounting root filesystem
kjournald starting. Commit interval 5 seconds
EXT3-fs: mounted filesystem with ordered data mode.
Switching to new root.
SELinux: Disabled at runtime.
SELinux: Unregistering netfilter hooks
audit(1201184700.838:2): selinux=0 auid=4294967295
INIT: version 2.85 booting
input: ImExPS/2 Generic Explorer Mouse as /class/input/input1
Setting default font (latarcyrheb-sun16):      [ OK ]

Welcome to ClarkConnect Community Edition
Press 'I' to enter interactive startup.
Iniciando el hardware...
```

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

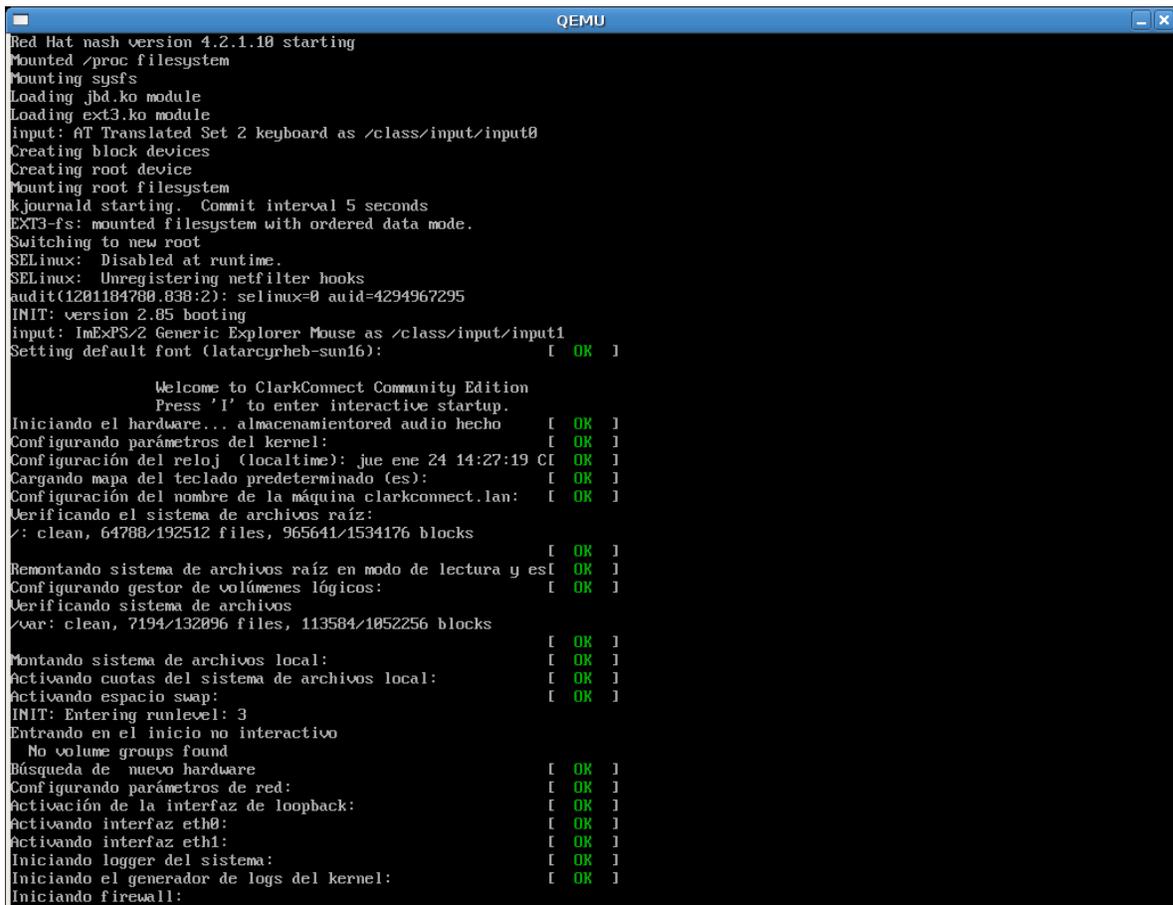
[Imagen 56]



```
QEMU
Initializing IPsec netlink socket
NET: Registered protocol family 1
NET: Registered protocol family 17
Using IPI No-Shortcut mode
Time: tsc clocksource has been installed.
Freeing unused kernel memory: 240k freed
Write protecting the kernel read-only data: 382k
Red Hat nash version 4.2.1.10 starting
Mounted /proc filesystem
Mounting sysfs
Loading jbd.ko module
Loading ext3.ko module
input: AT Translated Set 2 keyboard as /class/input/input0
Creating block devices
Creating root device
Mounting root filesystem
kjournald starting. Commit interval 5 seconds
EXT3-fs: mounted filesystem with ordered data mode.
Switching to new root
SELinux: Disabled at runtime.
SELinux: Unregistering netfilter hooks
audit(1201184780.838:2): selinux=0 audit=4294967295
INIT: version 2.85 booting
input: ImExPS/2 Generic Explorer Mouse as /class/input/input1
Setting default font (latarcyrheb-sun16): [ OK ]

Welcome to ClarkConnect Community Edition
Press 'I' to enter interactive startup.
Iniciando el hardware... almacenamientored audio hecho [ OK ]
Configurando parámetros del kernel: [ OK ]
Configuración del reloj (localtime): jue ene 24 14:27:19 C[ OK ]
Cargando mapa del teclado predeterminado (es): [ OK ]
Configuración del nombre de la máquina clarkconnect.lan: [ OK ]
Verificando el sistema de archivos raíz:
/: clean, 64788/192512 files, 965641/1534176 blocks [ OK ]
Remontando sistema de archivos raíz en modo de lectura y es[ OK ]
Configurando gestor de volúmenes lógicos: [ OK ]
Verificando sistema de archivos
/var: clean, 7194/132096 files, 113584/1052256 blocks [ OK ]
Montando sistema de archivos local: [ OK ]
Activando cuotas del sistema de archivos local: [ OK ]
Activando espacio swap: [ OK ]
INIT: Entering runlevel: 3
Entrando en el inicio no interactivo
No volume groups found
Búsqueda de nuevo hardware
```

[Imagen 57]



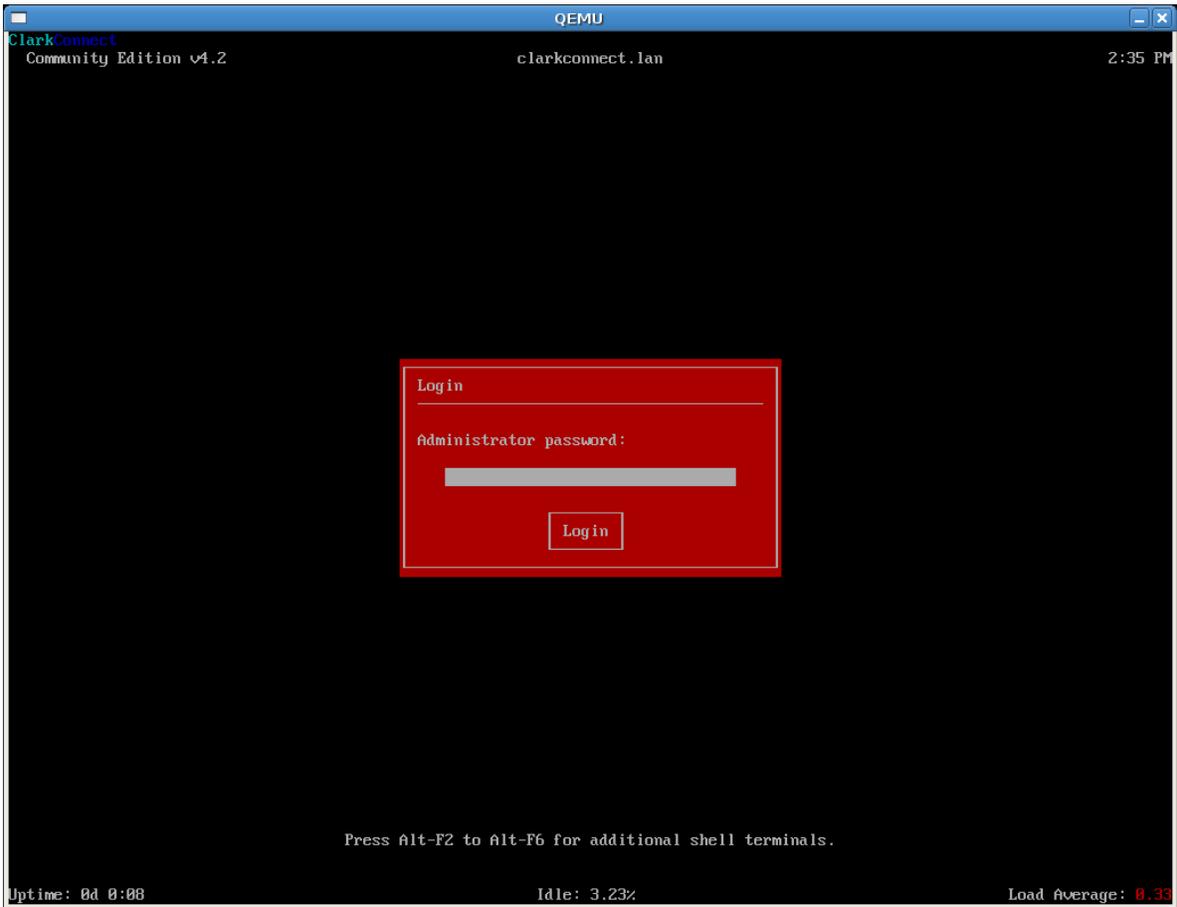
```
QEMU
Red Hat nash version 4.2.1.10 starting
Mounted /proc filesystem
Mounting sysfs
Loading jbd.ko module
Loading ext3.ko module
input: AT Translated Set 2 keyboard as /class/input/input0
Creating block devices
Creating root device
Mounting root filesystem
kjournald starting. Commit interval 5 seconds
EXT3-fs: mounted filesystem with ordered data mode.
Switching to new root
SELinux: Disabled at runtime.
SELinux: Unregistering netfilter hooks
audit(1201184700.838:2): selinux=0 auid=4294967295
INIT: version 2.85 booting
input: ImExPS/2 Generic Explorer Mouse as /class/input/input1
Setting default font (latarcyrheb-sun16): [ OK ]

Welcome to ClarkConnect Community Edition
Press 'I' to enter interactive startup.
Iniciando el hardware... almacenamiento de audio hecho [ OK ]
Configurando parámetros del kernel: [ OK ]
Configuración del reloj (localtime): jue ene 24 14:27:19 C [ OK ]
Cargando mapa del teclado predeterminado (es): [ OK ]
Configuración del nombre de la máquina clarkconnect.lan: [ OK ]
Verificando el sistema de archivos raíz:
/: clean, 64700/192512 files, 965641/1534176 blocks [ OK ]
Remontando sistema de archivos raíz en modo de lectura y es [ OK ]
Configurando gestor de volúmenes lógicos: [ OK ]
Verificando sistema de archivos
/var: clean, 7194/132096 files, 113584/1052256 blocks [ OK ]
Montando sistema de archivos local: [ OK ]
Activando cuotas del sistema de archivos local: [ OK ]
Activando espacio swap: [ OK ]
INIT: Entering runlevel: 3
Entrando en el inicio no interactivo
No volume groups found
Búsqueda de nuevo hardware [ OK ]
Configurando parámetros de red: [ OK ]
Activación de la interfaz de loopback: [ OK ]
Activando interfaz eth0: [ OK ]
Activando interfaz eth1: [ OK ]
Iniciando logger del sistema: [ OK ]
Iniciando el generador de logs del kernel: [ OK ]
Iniciando firewall:
```

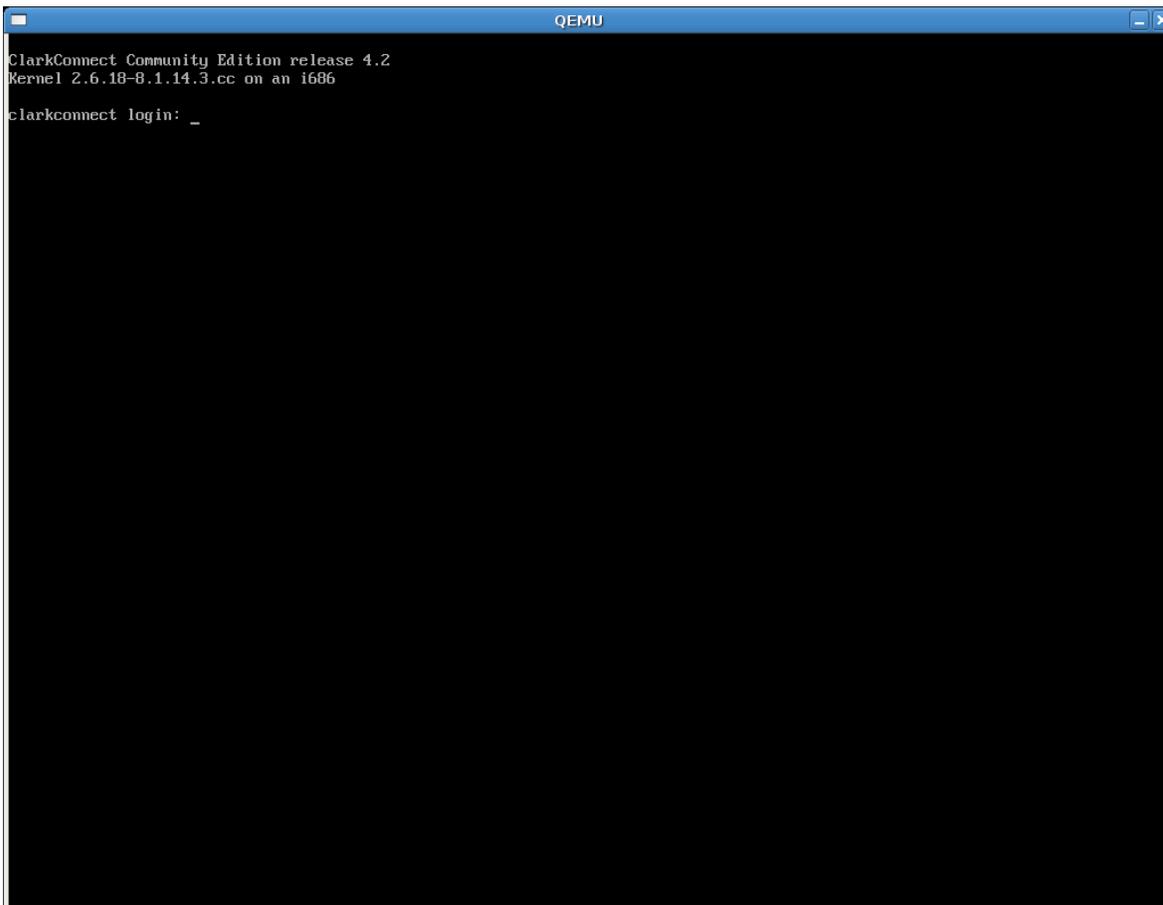
Dependiendo de la cantidad de módulos instalados en el servidor este tomará más, o menos tiempo en iniciar el sistema, cuando esto ocurra aparecerá un fondo negro junto con una pequeña ventana roja donde se pregunta por la contraseña del administrador del sistema (*root*). No es obligatorio ingresar al servidor por este camino, para usar una consola sólo se necesita presionar las teclas **Alt + Fx**, donde **x** es la consola número **x** del 2 al 6.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 58]



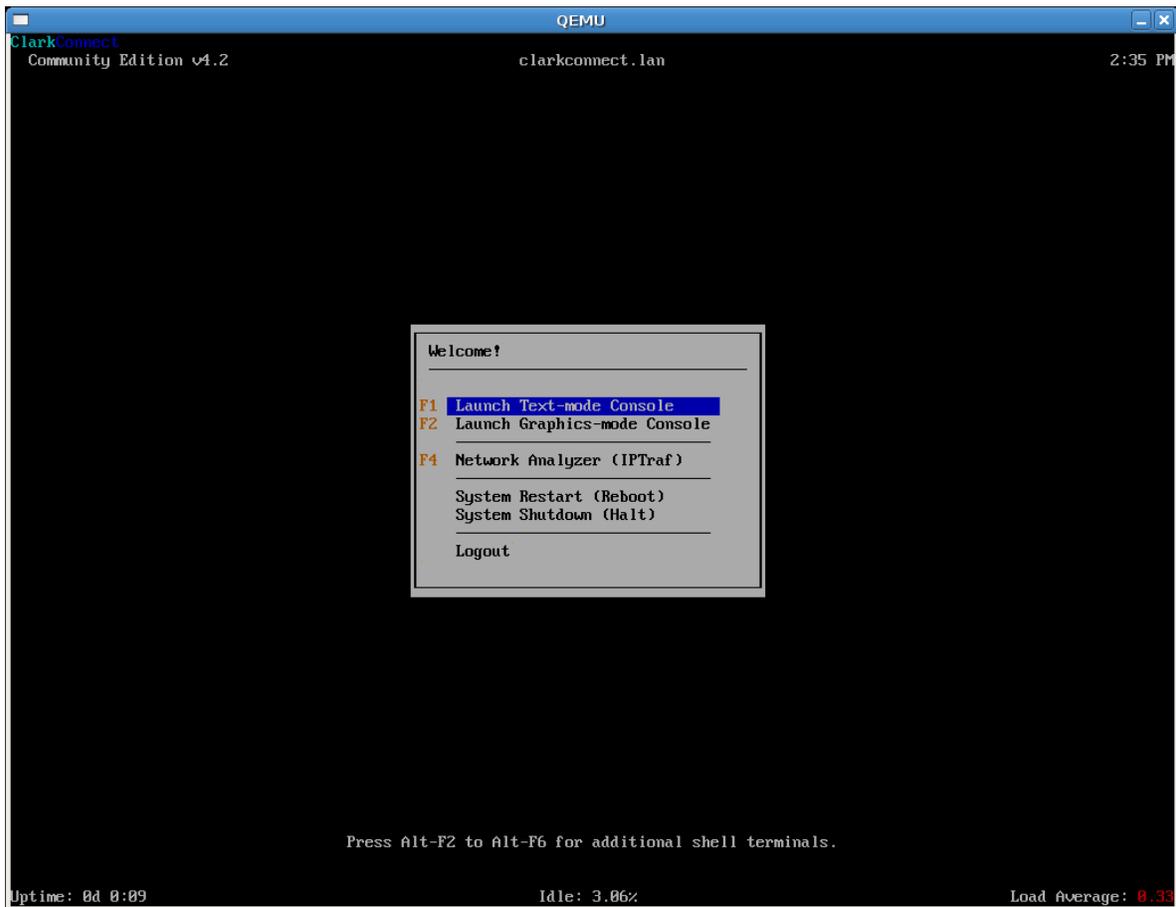
[Imagen 59]



Al escribir correctamente la contraseña ingresamos al sistema y nos muestra un menú con seis opciones. Escogeremos la opción que más convenga, en nuestro caso la consola gráfica (presionar F2) nos puede ser muy útil y fácil de usar.

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 60]



Cuando termine de cargar escribimos `Alt + F7` y esto nos lleva a la consola gráfica donde podemos revisar si la configuración de la red es la correcta o iniciar el servidor *DHCP*. Si no hay problemas la configuración primaria de la red se debe ver algo así:

```
eth0 External Ethernet Static IP PÚBLICA
```

```
eth1 LAN Ethernet Static IP SERVIDOR
```

De no ser así presionamos los iconos en forma de flechas a la izquierda del nombre de las interfaces de red (*eth0* - *eth1*) podemos configurar éstas como se requiera para su funcionamiento. La interfaz de la LAN es la más importante después de la instalación, ya que a través de ella ingresamos a la interfaz Web para configurar al servidor.

## **5.2 CONFIGURAR LAS INTERFACES DE RED**

Configurar las interfaces correctamente nos permitirá ingresar más fácil a Internet y a nuestra LAN. Ahora para configurar podemos elegir hacerlo desde la consola gráfica o bien ingresando a la pantalla inicial (**Alt+F1**) para editar la información en modo de texto.

Comenzamos seleccionando la primera interfaz *eth0*, con este nombre se designa a la primera tarjeta de red<sup>44</sup>. A continuación debemos seleccionar su rol en la red, esto es el papel que la interfaz desempeñará en la red como: *interfaz externa*, la cuál se conecta directamente al Internet; *interfaz para LAN*, esta es la que se conecta a la red interna de la institución; *Hot LAN*, este rol se usa para conectar la interfaz a redes locales (LAN) donde se sabe que existen máquinas en las que no

---

<sup>44</sup>En informática se comienza a contar normalmente a partir del número 0; así es en este caso.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

se confía (de su contenido), y se selecciona para redes inalámbricas ya que normalmente en estas cualquier computador se puede conectar; lo que finalmente se pretende con este rol es mantener a las máquinas confiables separadas de las que no lo son. El rol DMZ se usa habitualmente para ubicar servidores en un segmento separado de la red local y así aumentar la seguridad.

El tercer paso consta de escoger de qué tipo es la conexión, *Ethernet*, *Wireless* y *DSL/PPPoE*, las dos últimas se usan para conexiones que necesiten autenticación de algún tipo.

Continuamos con el protocolo que manejará la interfaz: *dinámico*, para conexiones a Internet a través de un módem o cuando se conecta a otro servidor que sirva *DHCP*; *estática* cuando se le quiere designar al servidor una *IP* fija, tanto para la *LAN* como para Internet.

Finalmente escribimos la dirección de *IP*, la máscara de red, la puerta de enlace y los servidores *DNS*, si escogimos el protocolo estático de lo contrario terminamos la configuración de red de las interfaces.

### **5.3.1 INTERFAZ WEB, INGRESO**

De ahora en adelante para administrar el servidor se necesita un computador conectado a la red *local*, en nuestro caso la: 192.168.1.0 .

Para configurar un computador con *Windows XP*® para pertenecer a esta *LAN* es necesario seguir estos pasos:

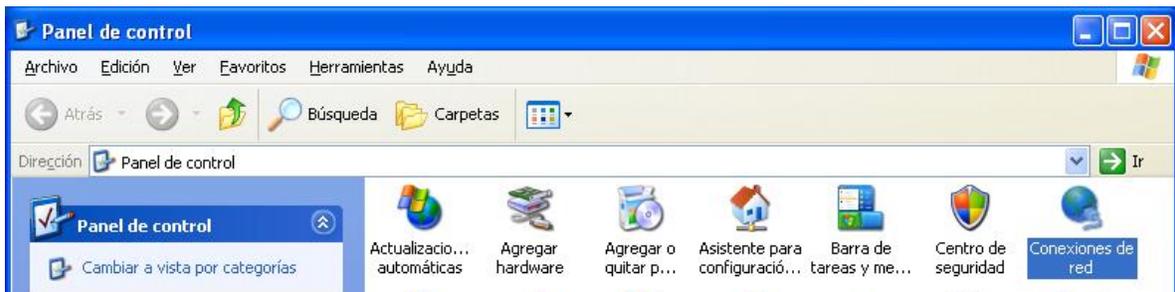
1. Seleccionar *Panel de Control* desde el menú de Inicio.
2. Hacer clic en *Conexiones de Red* desde el *Panel de Control*.
3. Escoger la conexión de la red *LAN*.
4. Clic en *Propiedades*.
5. Seleccionar *Protocolo de Internet (TCP/IP)* con un doble clic.
6. Se selecciona *Usar la siguiente dirección de IP* y escribimos lo siguiente:
  - Dirección de IP: 192.168.1.10 (los últimos dígitos puede ser cualquier número dentro del rango del 1-253).
  - Mascara de Subred: 255.255.255.0 .
  - Puerta de enlace: 192.168.1.254 , esta es la dirección de *IP* del servidor.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

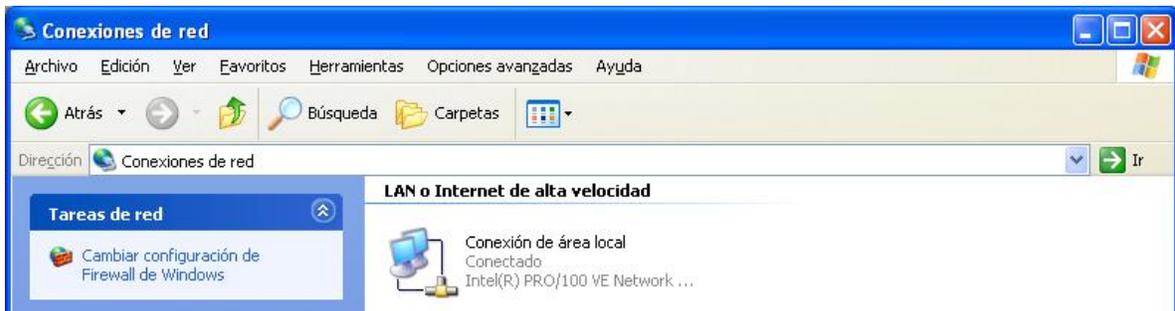
[Imagen 61]



[Imagen 62]



[Imagen 63]

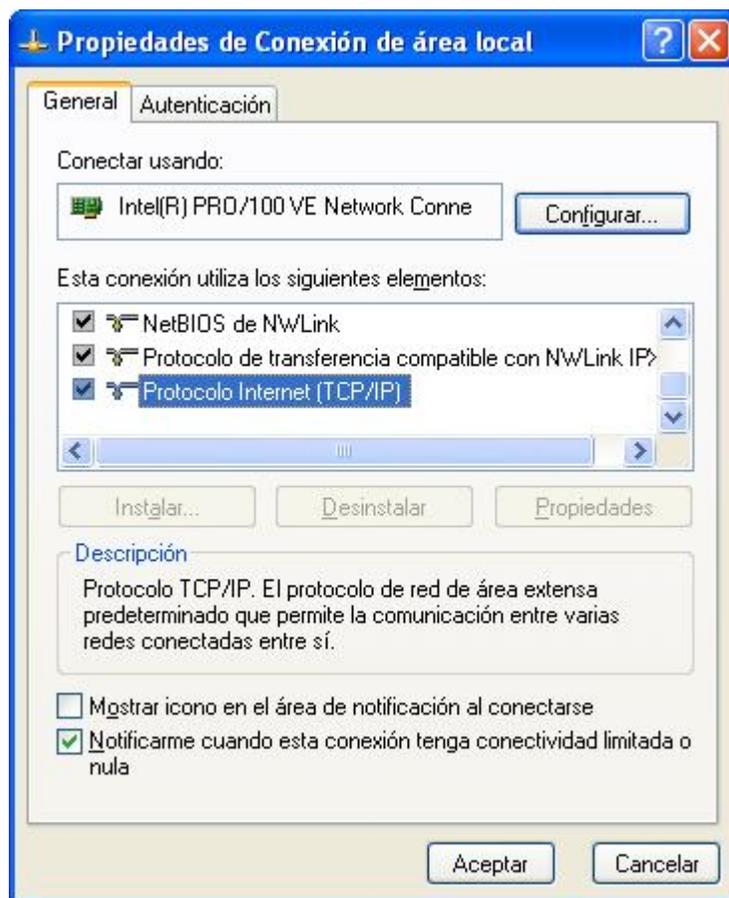


Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 64]



[Imagen 65]



Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

A continuación le damos clic a *reparar* en la conexión.

Si se activó la opción del *DHCP* en el servidor, se deben seguir los pasos anteriores, pero en vez de escoger la opción del paso 6 se escoge automático en ambas secciones. Realizado esto se abre una consola (en ejecutar escribir: *cmd.exe*) y se digita *ipconfig /renew* y esto actualizará la *IP* de la máquina por una que provee el servidor en el rango especificado.

[Imagen 66]

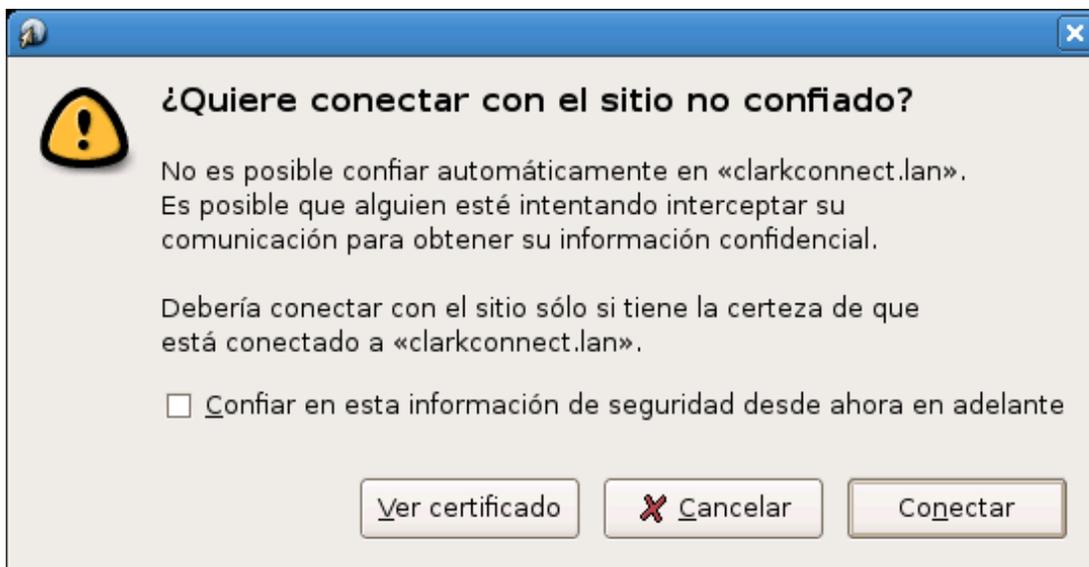


Abrimos un navegador y escribimos `https://192.168.1.254:81` y presionamos *Enter*. Ésta es la dirección para ingresar a la interfaz Web del servidor *ClarkConnect*.

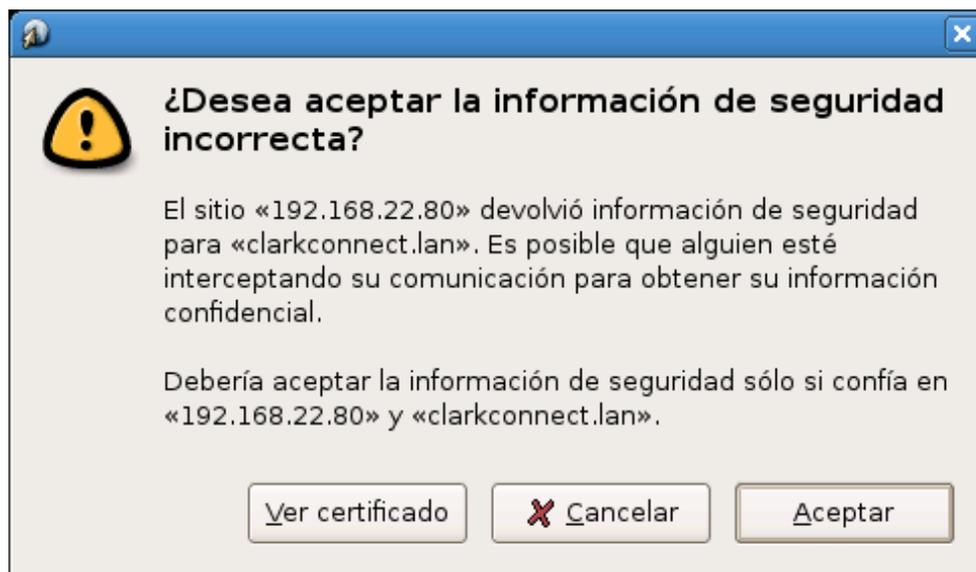
Lo que hacemos al escribir la dirección de esa manera es decirle al navegador que deseamos realizar una conexión segura si con el servidor con la dirección 192.168.1.254 y por el puerto 81. (Los servidores Web comunes usan el puerto 80 como estándar para comunicarse, pero para evitar confusiones y problemas de seguridad, en el *ClarkConnect* el

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar  
servicio de la interfaz Web se encuentra en el puerto 81).

[Imagen 67]

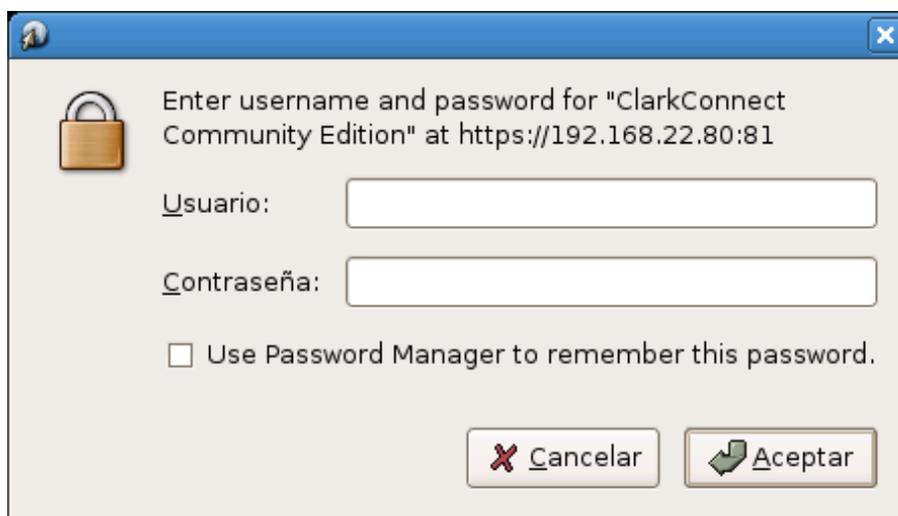


[Imagen 68]

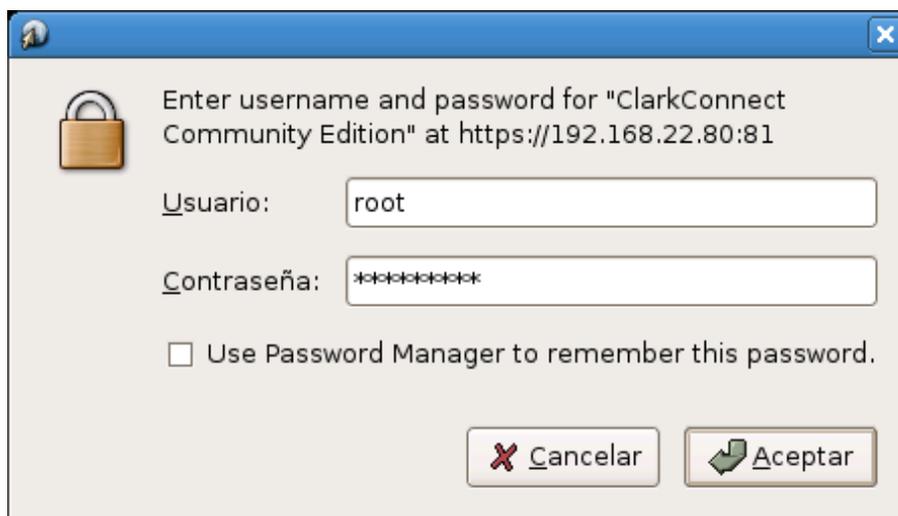


Durante la conexión el navegador pregunta si se desea conectar al servidor en cuestión, aceptamos y continuamos hasta que nos pregunten por el usuario y la contraseña. En usuario escribimos `root` y la contraseña correspondiente.

[Imagen 69]



[Imagen 70]



Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

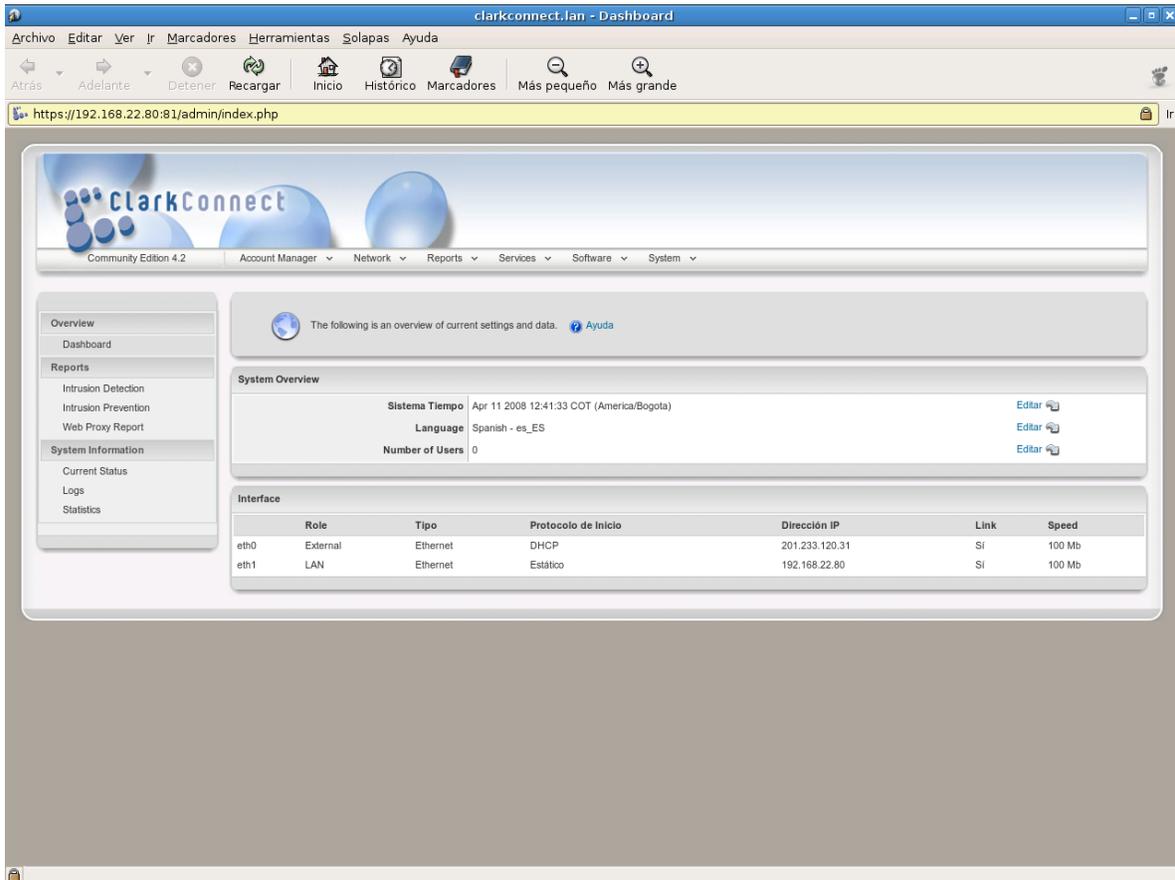
Se recomienda evitar escoger la casilla para recordar la contraseña por cuestiones de seguridad.

A continuación comienza a cargar la página inicial de la interfaz Web del servidor, donde nos muestra brevemente algunos datos sobre el servidor y la red donde se encuentra.

### **5.3.2 CONFIGURACIÓN FINAL DE LA RED**

Al ingresar a la interfaz Web de configuración (en adelante *Webconfig*) se muestra un “tablero” (*Dashboard*) con algunos de los datos más importantes y relevantes del servidor, como la configuración del idioma, la hora y el estado y las características de las interfaces de red. Adicionalmente, si se tiene instalado el módulo de prevención de intrusos muestra una lista con las últimas detecciones.

[Imagen 71]

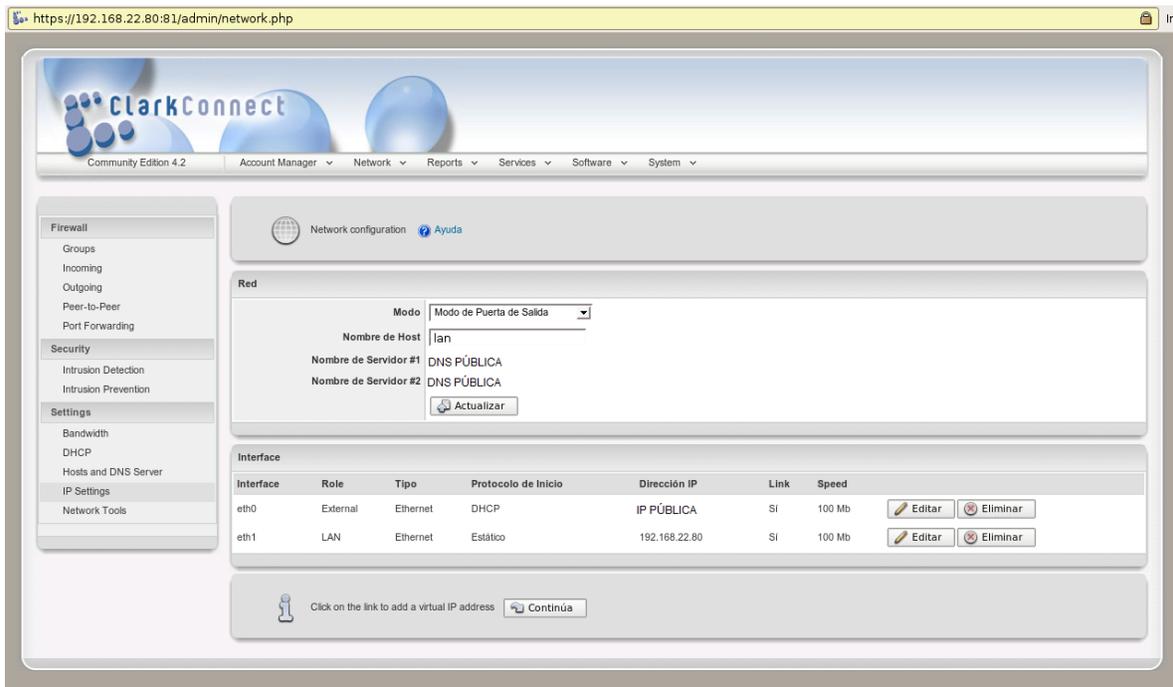


**Nota:** es recomendable mantener el idioma de preferencia en inglés, ya que de esta forma se tendrá una idea más clara de las opciones que nos brinda el *ClarkConnect*.

Para este momento las interfaces de red ya deben estar correctamente configuradas, pero puede que sean necesarios algunos ajustes o correcciones, en este apartado examinaremos eso.

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 72]



Nos vamos a la pestaña `Network` y seleccionamos `IP Settings`. Esto nos lleva a una página que nos permite modificar la configuración de la red. Vemos una menú desplegable para escoger el modo como queremos que funcione nuestro *ClarkConnect*. Como nuestra finalidad es que el servidor funcione como *Firewall* y como *Proxy* para la red, seleccionamos `Gateway Mode`; de lo contrario las dos opciones restantes son similares. Como su nombre lo dice le dan la condición al servidor de prestar servicios en una red o Internet, pero sin tener la función de “ruteador” de red o de *Proxy*.

En `hostname` aparece el nombre que le dimos a la máquina junto con la red a la que pertenece, por ejemplo:

clarkconnect.lan

óó

ccsrv.colegioalemanmedellin.edu.co

Éste se puede cambiar de ser necesario a un nombre mas descriptivo, corto y sencillo, pero manteniendo su forma de escritura: nombre\_de\_la\_máquina.dominio (clarkconnect.lan). Para hacer efectivo algún cambio realizado se necesita pulsar el botón Update. ¡Esto mismo se debe realizar cuando se modifique alguna opción en el *Webconfig!*, de lo contrario no se realizarán los cambios.

Seguimos bajando y vemos la lista de los servidores *DNS* a los que consulta nuestro servidor para las peticiones Web externas, estos son los mismos que se configuraron en la interfaz de red externa en los apartados 5.1 y 5.2. Si es necesario a través de la consola se pueden modificar manualmente estos *DNS*, esto puede ser muy conveniente para diferentes usos. Para realizar esto, ingresamos en una consola bien sea local o remotamente, ¡si de desea hacerlo remotamente leer el apartado 5.3.5 previamente!, y ejecutamos la siguiente orden como superusuario:

```
nano /etc/resolv.conf
```

Lo que se hace con este comando es modificar el archivo *resolv.conf*, el cual guarda las direcciones de los *DNS*, ubicado en */etc* con el programa de edición de texto *nano*. *Nano* es un programa sencillo pero útil; nos movemos con los cursores a la línea que deseamos modificar y borramos o escribimos lo que necesitamos.

El archivo de texto se ve algo así:

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

```
search dominio.com
nameserver 192.168.0.250
nameserver 192.168.0.251
```

Para modificarlo se necesita simplemente cambiar la dirección de *IP* del servidor *DNS*. Yo recomiendo en vez de borrar, comentar la línea para que no sea tomada en cuenta y luego escribir los servidores que deseamos. El símbolo *#* se usa al inicio de una línea para comentarla, así que el contenido de la línea, sin importar el que sea, será ignorado.

El archivo final quedaría algo así:

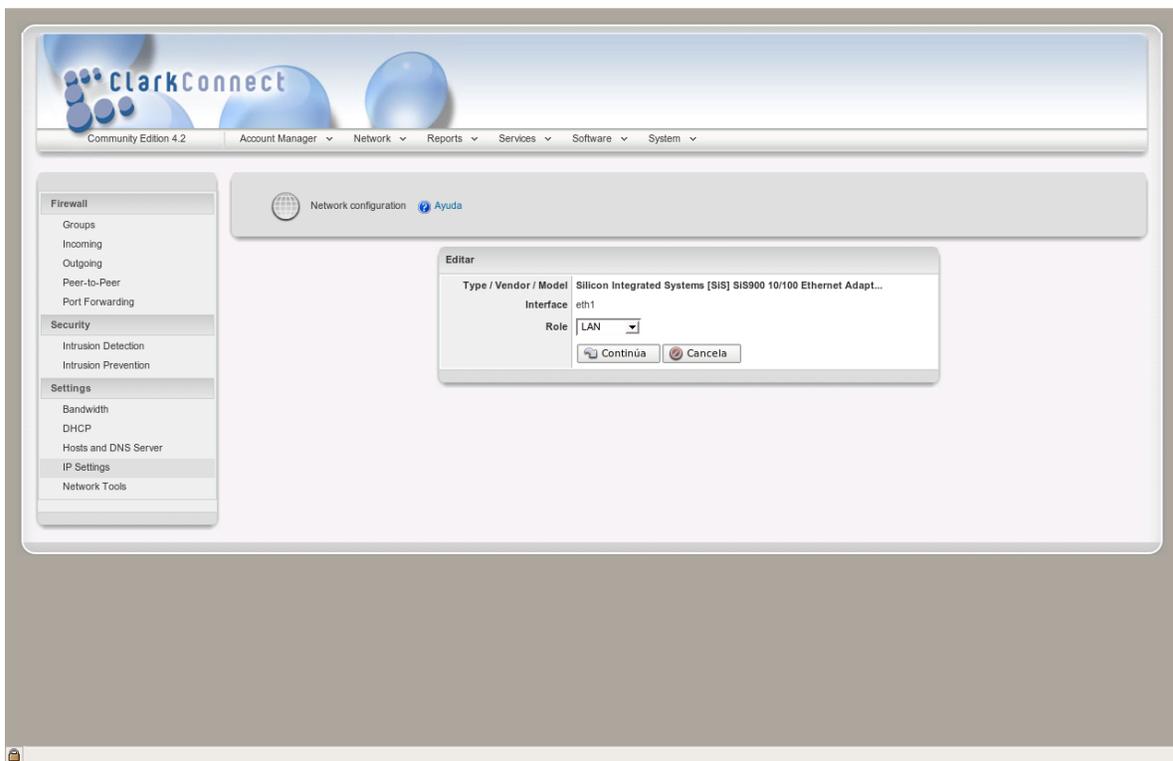
```
#search dominio.com           línea comentada
#nameserver 192.168.0.250     línea comentada
nameserver 192.168.0.251
nameserver 192.168.0.252     #nuevo servidor DNS
```

En la sección inferior de la consola se muestran las opciones y acciones que se pueden realizar con las combinaciones de teclas, por ejemplo salir: si se realizó algún tipo de cambio en el archivo cuando tecleemos *Ctrl + x*, el programa preguntará si se desean guardar los cambios realizados, nuevamente *Nano* nos muestra qué podemos hacer en este caso; como deseamos guardar los cambios y salir del programa

presionamos 'y' (seguido de la tecla *Enter*); de lo contrario se presiona 'n'.

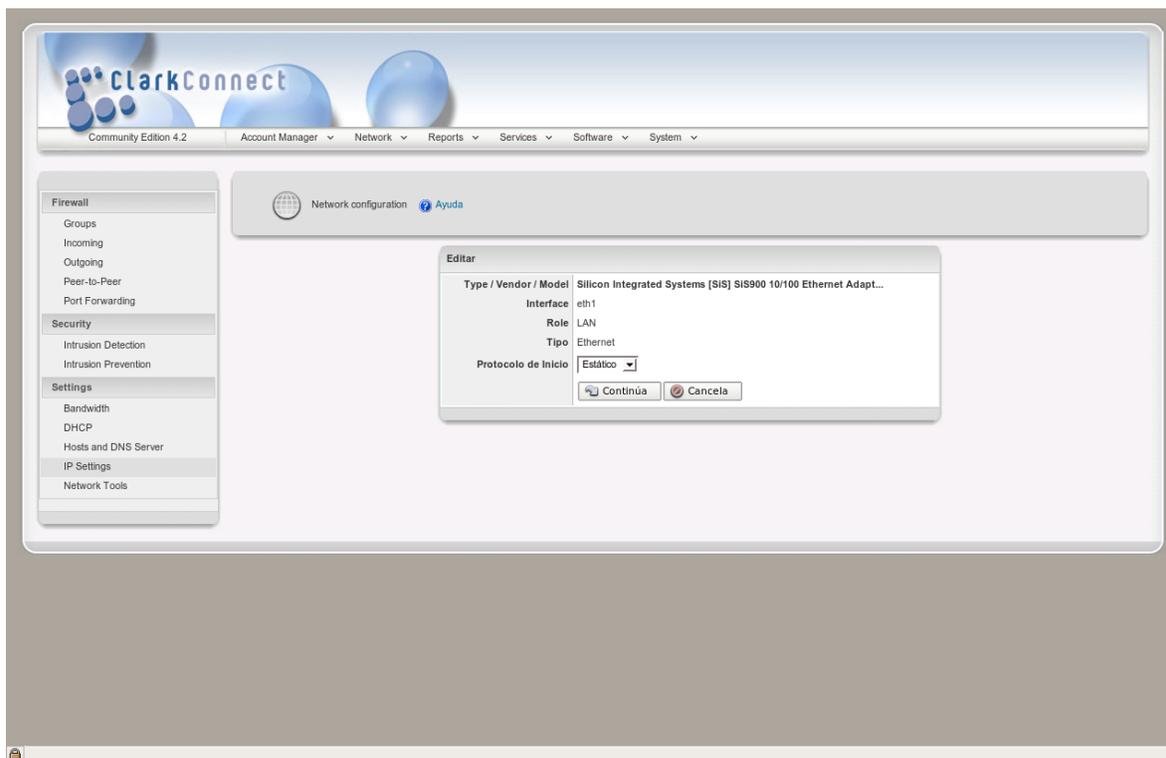
Más abajo de la sección donde se muestran los servidores *DNS*, se ve la misma tabla con las interfaces que se muestran en el *Dashboard*, sólo que en este caso podemos modificar la configuración de las interfaces, casi de igual forma como se hace en los apartados 5.1 y 5.2.

[Imagen 73]

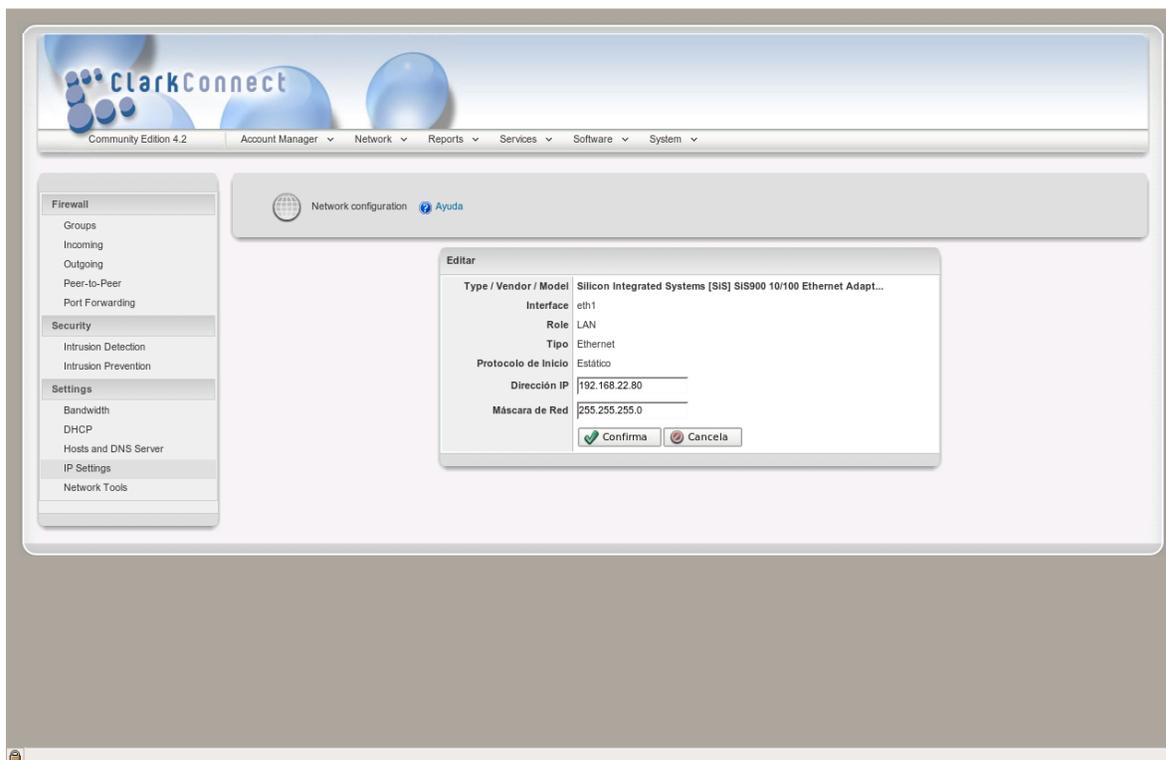


## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 74]



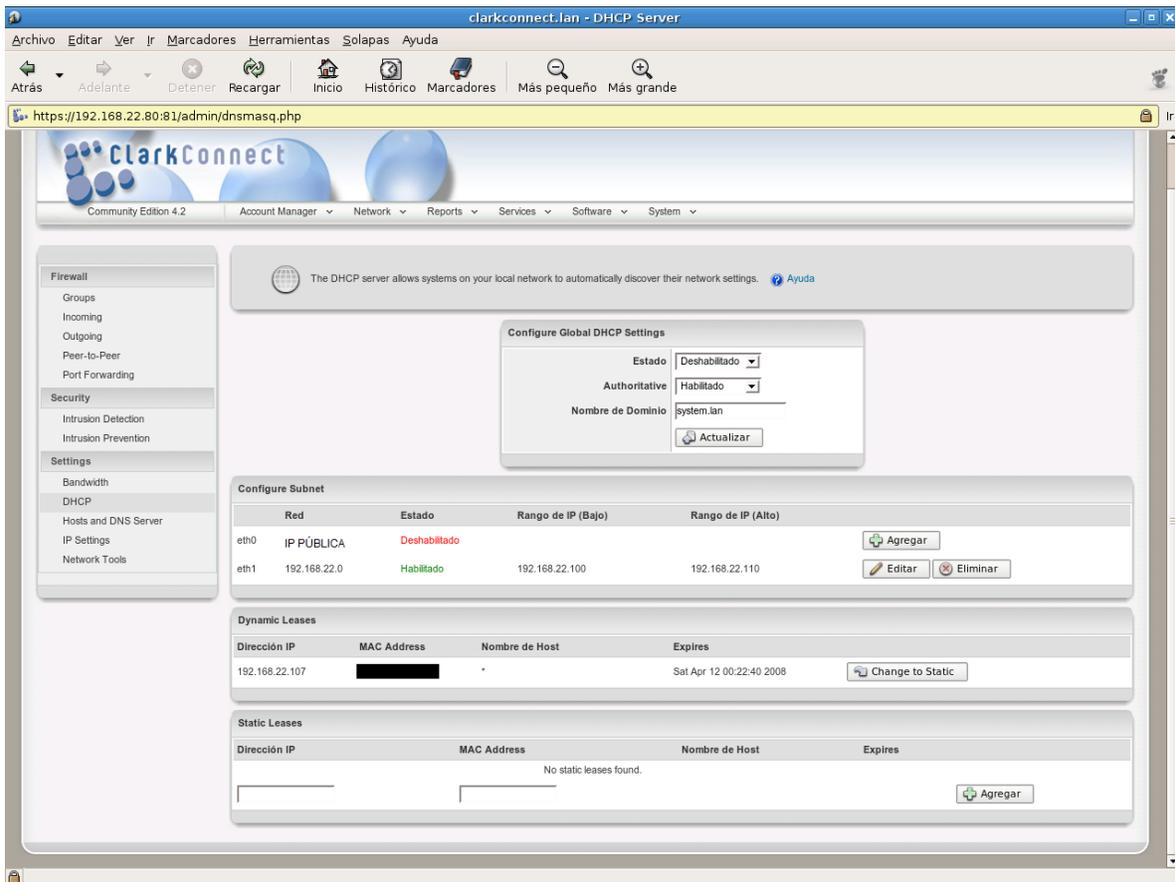
[Imagen 75]



Por el momento no nos interesa hacer conexiones de tipo *VPN* a otras redes así que podemos continuar con otro aspecto importante en la configuración de una red *LAN*, el *DHCP*. Para ir a la página del *DHCP* podemos seleccionarla de la columna de la izquierda, o bien como se llegó a la de *Network* por las pestañas.

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 76]



En la sección *Configure Global DHCP Settings*, se modifican las configuraciones globales de este servicio. Para encenderlo le cambiamos el *Status* a *Enabled*. La segunda opción se llama *Authoritative* y si está habilitada el servidor aceptará todas las peticiones *DHCP* que lleguen a la red, aunque en ella existan otros dispositivos que puedan servir *DHCP*. En *Domain Name* aparece el dominio de la red al cual pertenece nuestro *ClarkConnect*, por ejemplo:

lan  
ejemplo.com

[Imagen 77]

clarkconnect.lan - DHCP Server

Archivo Editar Ver Ir Marcadores Herramientas Solapas Ayuda

Atrás Adelante Detener Recargar Inicio Histórico Marcadores Más pequeño Más grande

https://192.168.22.80:81/admin/dnsmasq.php

ClarkConnect  
Community Edition 4.2 Account Manager Network Reports Services Software System

The DHCP server allows systems on your local network to automatically discover their network settings. Ayuda

Configure Global DHCP Settings

Estado: Habilitado  
Authoritative: Habilitado  
Nombre de Dominio: system.lan  
Actualizar

Configure Subnet

Red	Estado	Rango de IP (Bajo)	Rango de IP (Alto)	
eth0	IP PÚBLICA	Deshabilitado		Agregar
eth1	192.168.22.0	Habilitado	192.168.22.100	192.168.22.110 Editar Eliminar

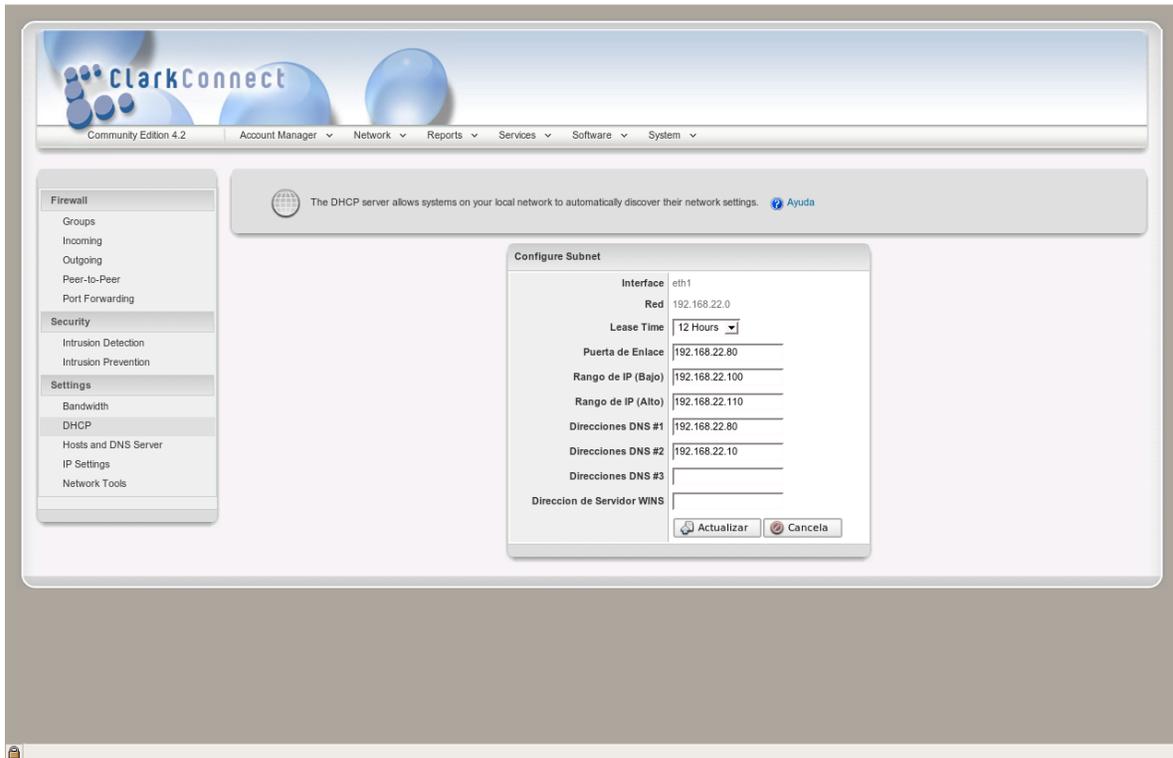
Dynamic Leases

Dirección IP	MAC Address	Nombre de Host	Expires	
192.168.22.107		*	Sat Apr 12 00:22:40 2008	Change to Static

Static Leases

Dirección IP	MAC Address	Nombre de Host	Expires	
No static leases found.				Agregar

[Imagen 78]



En la siguiente sección se configura una subred, a la cual está asociada una tarjeta de red. Por ejemplo: la interfaz *eth1* se encuentra en la red 192.168.1.0 . Esto significa que a esta red es a la que le podemos brindar el servicio *DHCP*. Si se desea tener en más de una red este servicio, se requiere por cada red adicional una interfaz más. Presionamos en **Add** y nos lleva a una ventana donde podemos configurar las opciones que deseamos que tenga el *DHCP*. Para comenzar seleccionamos el tiempo que el servidor le presta a cada dispositivo una dirección de *IP*. Bajamos un poco y especificamos el *Gateway*, este es el dispositivo, en este caso el servidor *ClarkConnect*, por el cual salen las conexiones a Internet, en este campo, como en los

siguientes se escriben direcciones de *IP*. Continuando, llegamos a los rangos en los cuales el servidor repartirá las direcciones, se especifica el rango más bajo y más alto dentro de la red de la interfaz. Seguidamente los servidores *DNS*, aquí se especifican las máquinas (servidores) a los cuales deben llegar las peticiones *DNS* para navegar en Internet o en la red local. Si se tiene en la red un servidor *DNS* se debe especificar su dirección de *IP* aquí mismo, de lo contrario se escribe dirección del servidor *ClarkConnect* que da la salida a Internet. Finalmente, la dirección del servidor *WINS*, este servidor se encarga de mantener una “base de datos de direcciones IP y nombres de ordenador que se actualiza dinámicamente según cambian las direcciones IP<sup>45</sup>” para asociar un nombre a una dirección de *IP*. Este servidor existe dentro de grandes redes donde coexisten muchos servidores o máquinas con nombres específicos a los cuales es necesario acceder continuamente para diferentes tareas, como almacenamiento de archivos, en estos casos es muy difícil e incomodo memorizarse todas las direcciones de *IP* de cada máquina, una máquina que sirva *WINS* es la solución a esto.

---

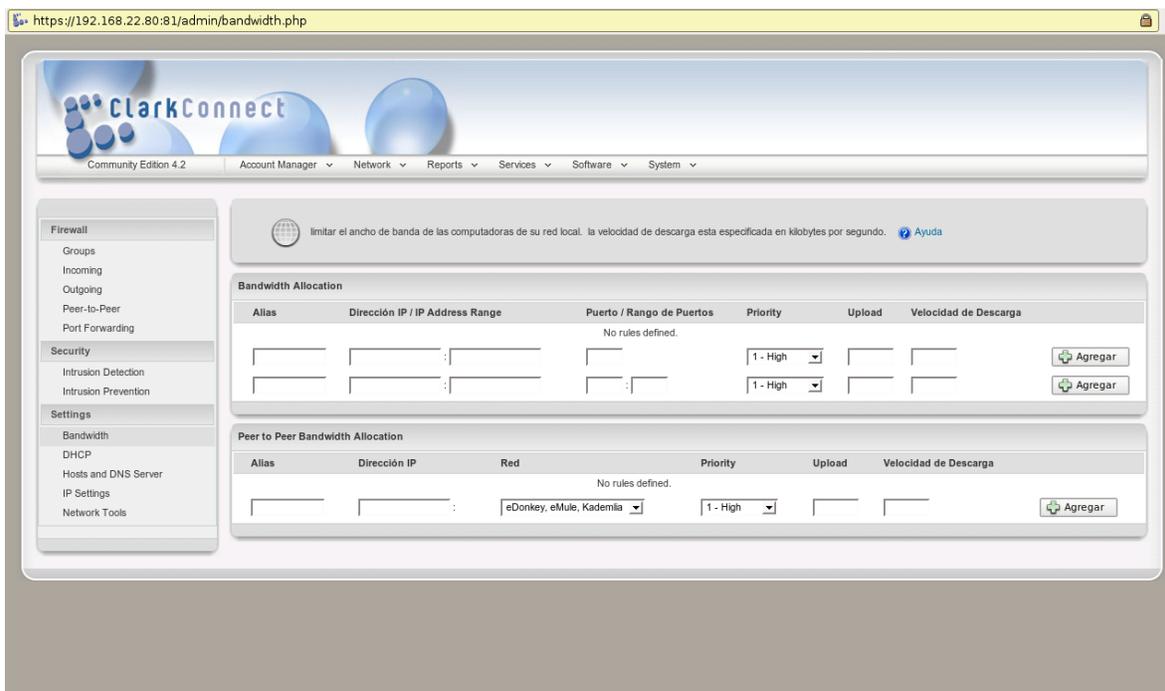
45 Cita de: <http://bc.inter.edu/facultad/lcardona/InfGen/WINS&DNS.htm>

El esquema final de las características del *DHCP* se vería así:

<i>Interface</i>	<i>eth1</i>
<i>Network</i>	<i>192.168.1.0</i>
<i>Lease Time</i>	<i>12 Hours</i>
<i>Gateway IP Range (low)</i>	<i>192.168.1.2</i>
<i>IP Range (high)</i>	<i>192.168.1.130</i>
<i>DNS Address #1</i>	<i>192.168.1.254</i>
<i>DNS Address #2</i>	<i>[vacío]</i>
<i>DNS Address #3</i>	<i>[vacío]</i>
<i>WINS Server Address</i>	<i>[vacío]</i>

En la sección que continúa, *Dynamic Lease* se puede conocer qué máquina (a través de su dirección *MAC* y su nombre de red) está asociada a qué *IP*. Y si se prefiere, esta asociación se puede volver estática, esto significa que no importa cuantas veces una máquina asociada se conecte a la red, siempre tendrá la misma dirección de *IP*. Esto puede ser útil para saber qué máquina tiene cierta *IP*, pero a gran escala puede ser muy difícil de mantener. Adicionalmente, se pueden añadir máquinas manualmente, especificando una dirección de *IP* que no esté en uso y una dirección *MAC* única.

[Imagen 79]



Para garantizar que el servidor pueda usar el ancho de banda que necesita según el caso, nos dirigimos a la sección Bandwidth. Aquí, por medio de sencillos parámetros, se reserva un ancho de banda para una máquina o un conjunto de ellas. En *Nickname* se escribe un nombre o apodo que la nueva regla tendrá, seguido de una dirección de *IP* o un rango de éstas, para el rango se escribe:

*192.168.1.100: 192.168.1.150*

Seguido se especifican un número o un rango de puertos, si no se especifica nada en estos cuadros de texto a todos los puertos se aplicará esta regla. *Priority* proporciona una forma para priorizar el tráfico de la

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

red. Al tráfico con mayor prioridad se le dará preferencia sobre el tráfico de menor prioridad. Existen siete niveles de prioridad, 1 - 7, donde uno es el de más alta prioridad. Por defecto el tráfico que no tenga una regla de ancho de banda se le asignará la prioridad más baja. Finalmente, se selecciona cuánto ancho de banda de subida (*upload*) y de bajada (*download*) se desea reservar para la nueva regla. Si se deja en blanco alguno de los dos, el ancho de banda de subida o bajada será ilimitado<sup>46</sup>, pero sólo se puede realizar en uno de los campos, si se dejan los dos en blanco la regla será inválida.

Las opciones que no se vieron o trabajaron en este capítulo serán vistas mas adelante cuando se llegue a una configuración mas avanzada del *Firewall*. Ahora que se terminó de configurar la red, podemos continuar con el siguiente apartado.

---

<sup>46</sup> El Ilimitado se refiere al ancho de banda permitido por la conexión de red o de Internet.

### **5.3.3 Proxy SERVER**

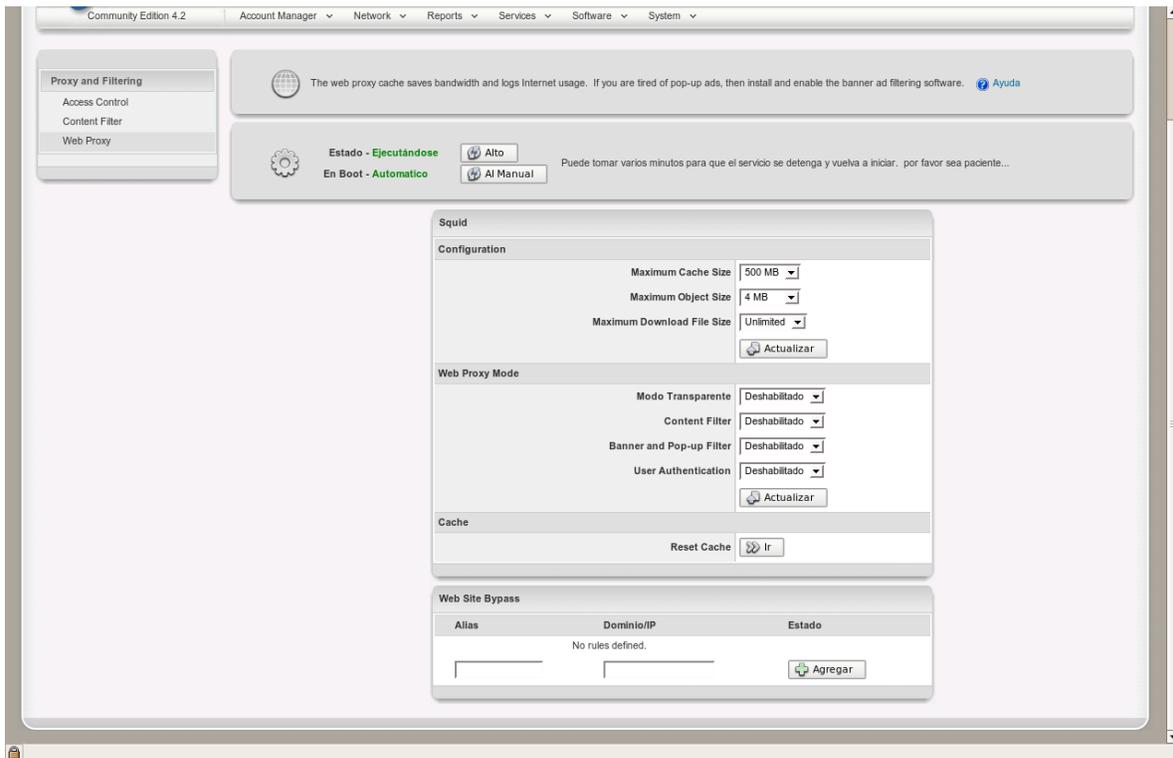
El servidor tiene un servicio de *Proxy* que se usa para que varios clientes puedan conectarse a la red a través de una única conexión física a Internet. Éste puede permitir, denegar o filtrar el contenido y el uso del Internet en la red, es decir, como un cuello de botella por donde pasan todas las conexiones al exterior. Pero adicionalmente el **Proxy**, llamado *Squid*, realiza un caché<sup>47</sup> de las páginas que se visitan para así aumentar la velocidad con que se navega en Internet, evitando cargar directamente del Internet siempre el mismo contenido; *Squid* almacena el contenido en un espacio asignado del disco duro, para que cuando los usuarios lo requieran simplemente sea transmitido en la red local, evitando usar parte del ancho de banda de la conexión a Internet.

---

<sup>47</sup> Son datos que fueron duplicados de los originales, debido a que los datos originales son costosos de acceder, en tiempo y otros factores, con respecto a la copia existente en el caché. Al acceder por vez primera a un dato, se le hace una copia en el caché, los accesos que siguen al primero se realizan a dicha copia, haciendo que el tiempo de acceso a los datos sea menor.

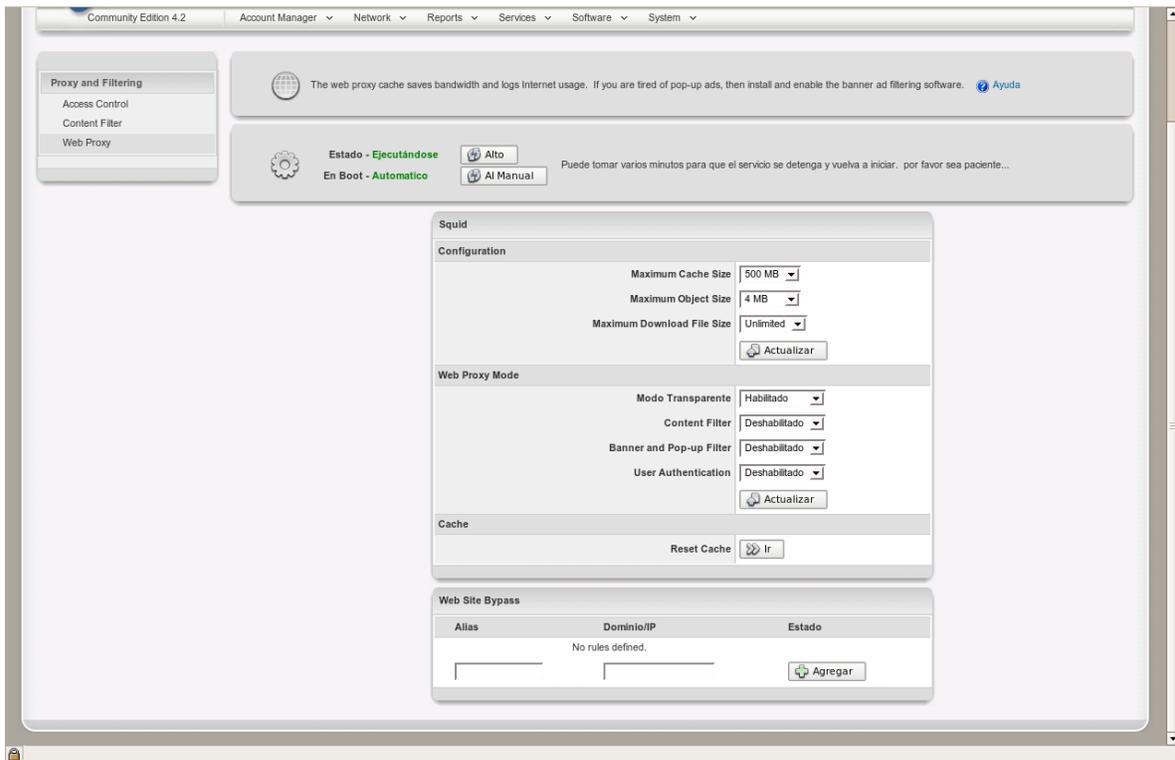
## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 80]



En la sección superior de la página se puede ver una breve descripción del servicio, es muy útil leerlo para informarse mejor de lo que realiza. Más abajo, nos encontramos con una pequeña pero importante sección que nos muestra el estado actual del servicio y el estado durante el inicio del sistema. *Running* (corriendo) y *Stopped* (detenido) son los estados en los que se encuentra y se pueden modificar con el botón al lado derecho. De igual forma funciona el otro estado del servicio durante el inicio, lo único que cambia es el modo Automático o Manual. Este método para saber el estado de los servicios corriendo en el servidor, se usa para la mayoría del *software*, módulos y servicios instalados en el servidor, es simple e intuitivo.

[Imagen 81]



Para configurar el *Proxy*, modificamos el espacio deseado para el caché, que puede ser desde los 100 *MB* hasta los 500 *GB*. Entre más espacio disponible menos páginas se tendrán que cargar de Internet. Continuamos con el tamaño máximo que tendrá cada objeto en el caché, puede ser una imagen, una página Web u otro tipo de archivo o contenido, es recomendable tener un tamaño razonable, algo así como 5 o 10 *MB*, archivos con tamaños mayores pasarán a través del *Squid* pero no serán guardados en la memoria caché. La siguiente opción da la posibilidad de escoger que tamaño máximo puede tener una descarga de Internet. Esto puede ser útil para evitar la descarga de grandes archivos como películas o imágenes de *CD* (archivos *\*.iso*, *\*.bin*, *\*.nrg*,

\*.img y \*.mdf). Para hacer efectivos los cambios realizados pulsamos el botón de Update.

Ahora configuramos el modo en que el *Proxy* actuará en la red. Si se escoge el modo transparente (*Transparent Mode*) el *Proxy* interceptará todo el tráfico Web que fluya por la red. En este modo no es necesario configurar los navegadores para que naveguen a través del *Squid*, pero dado la naturaleza del protocolo, páginas de Web seguras (*HTTPS*) no pasarán a través del *Proxy*. Es recomendable desactivar este modo, así la red, y por ende la navegación en Internet, será un poco más segura, además de obtener otros beneficios adicionales como autenticación de usuario (sólo si se habilita ese modo). De forma similar funciona el módulo de control de contenido (*Content Filter*), el cual si está activado (*Enabled*), filtra el tráfico que pasa por el *Squid* buscando contenido no permitido o peligroso y bloqueando su acceso a y desde la red. Por el momento es mejor desactivar (*Disabled*) esta opción hasta que el módulo de control de contenido esté correctamente configurado.

Para filtrar *banners* de publicidad y ventanas emergentes (*Banner and Pop-up Filter*) se activa la opción por `Enabled`.

La ultima opción de esta sección se puede ignorar, aunque es útil para conocer y restringir el acceso a diferentes usuarios, en una red de más de 100 usuarios se complica mucho el uso del modo de *User Authentication*; adicionalmente el *ClarkConnect 4.2 Community* solo permite tener hasta 10 usuarios registrados en el servidor sin cargo adicional, para aumentar esta cantidad se requiere pagar 20 USD<sup>48</sup> por cada usuario adicional que se quiera agregar. Se presiona Update y continuamos.

---

<sup>48</sup> Este valor puede variar con el paso del tiempo.

Si presionamos en *Go* se borraría todo el caché del *Squid* que esté guardado actualmente en el disco duro, es recomendable realizarlo una vez cada semana para limpiar el disco duro.

La sección de *Web Site Bypass* permite a los dominios o direcciones de *IP* seleccionadas, atravesar el *Proxy* sin pasar por el filtro o alguna otra medida que realice el *Squid*. Esto puede ser útil si algún tipo de servicio o dispositivo en la red no puede acceder a contenido en Internet al existir un *Proxy* en medio. Para hacer esto se escribe un apodo o nombre para describir la regla, en la siguiente casilla se escribe el dominio o el rango y finalmente se presiona *Add*.

Después de finalizar la configuración del *Proxy*, procedemos a configurar el navegador y programas adicionales que necesiten entrar a Internet (a través de un *Proxy*). Si se escogió el modo transparente, el navegador no necesita configuración para navegar sin problemas en Internet. De lo contrario, se debe configurar el navegador de preferencia.

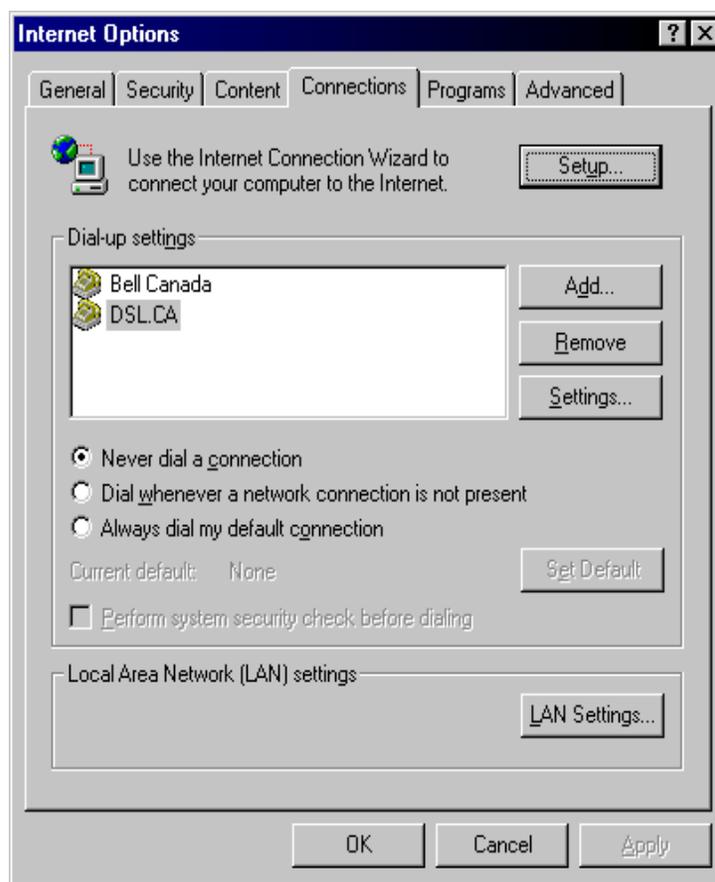
### **5.3.3.1 PASOS PARA CONFIGURAR MS INTERNET EXPLORER®**

Los pasos descritos a continuación muestran como configurar el *Internet Explorer®* de *Microsoft*, si se conoce como realizar esta sencilla operación, se puede saltar este apartado.

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

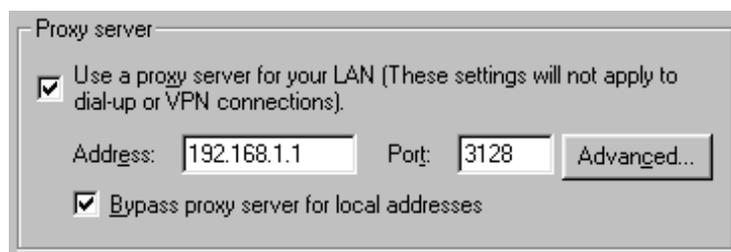
- Dar clic en Herramientas en el menú
- Seleccionar Opciones de Internet
- Clic en la pestaña Conexiones
- En la parte inferior dar clic en Propiedades de LAN

[Imagen 82]



En la sección del Servidor *Proxy*, se da clic en el *checkbox* para modificar la dirección del servidor *gateway*, en este caso el *ClarkConnect* (192.168.1.254), seguido del puerto al cual se dirigen las conexiones. Por defecto, el puerto 3128 es el designado si no se activó el filtro de contenido, de lo contrario el puerto sería 8080.

[Imagen 83]



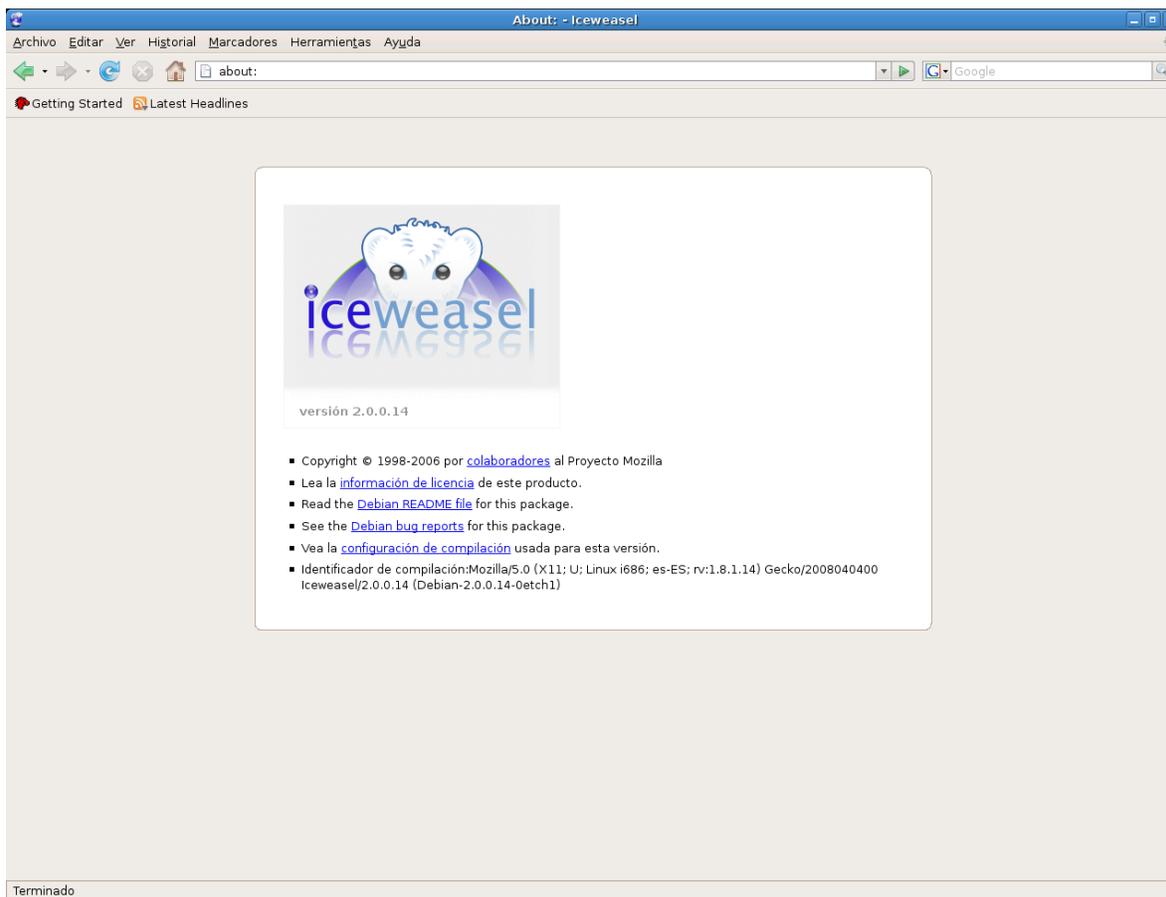
### 5.3.3.2 PASOS PARA CONFIGURAR MOZILLA FIREFOX®

- Dar clic en Herramientas en el menú
- Seleccionar Preferencias
- Clic en Avanzado
- Seleccionar la pestaña Red

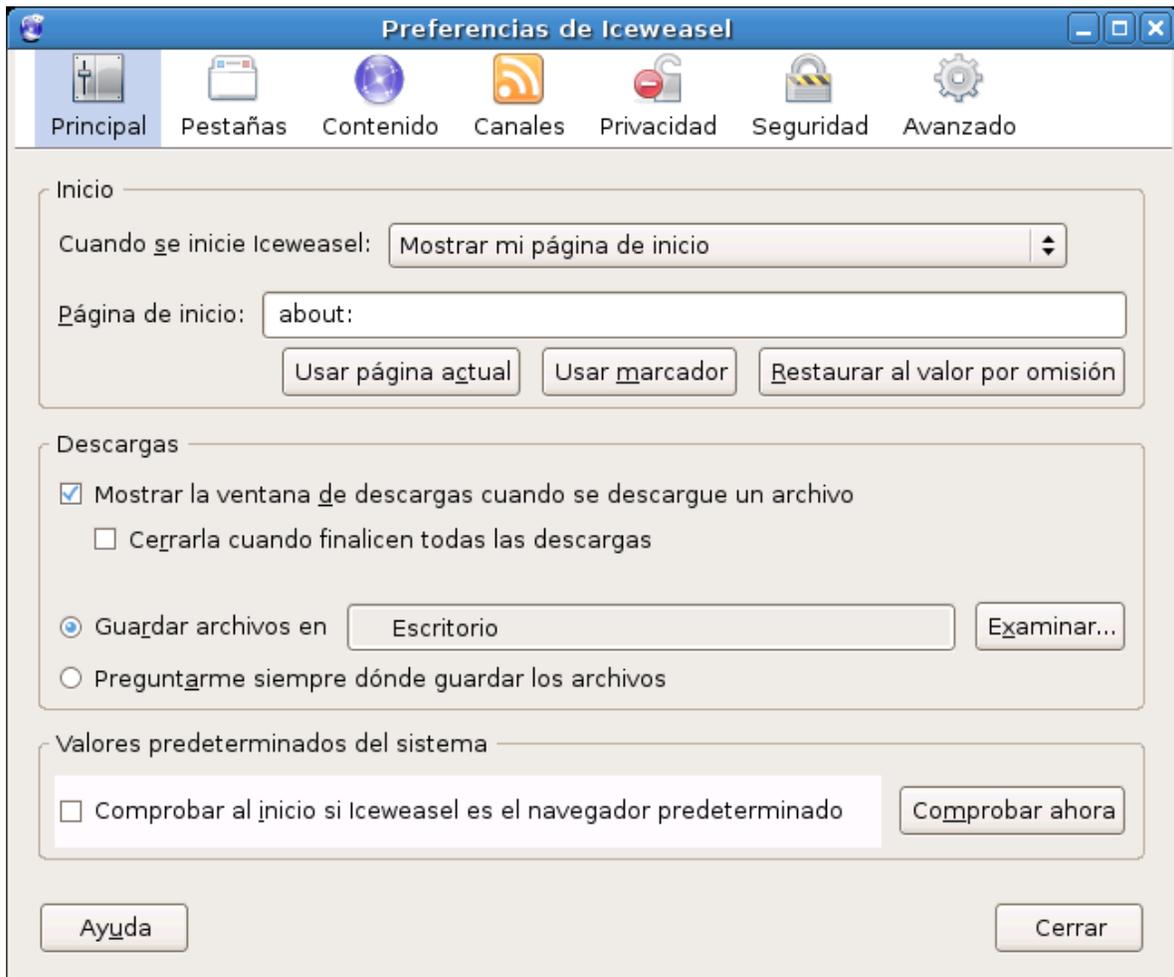
## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

- Hacer clic en Configuración...

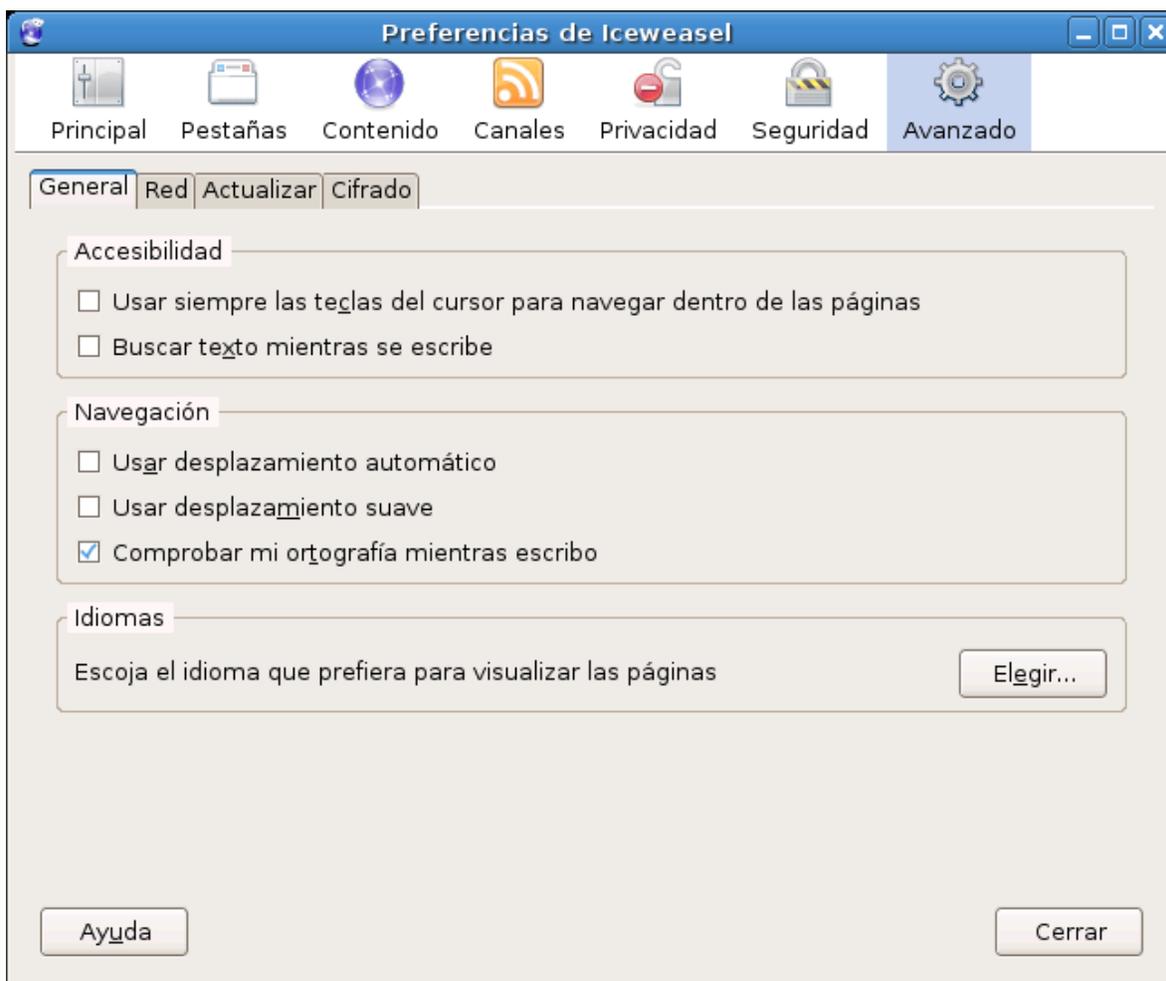
[Imagen 84]



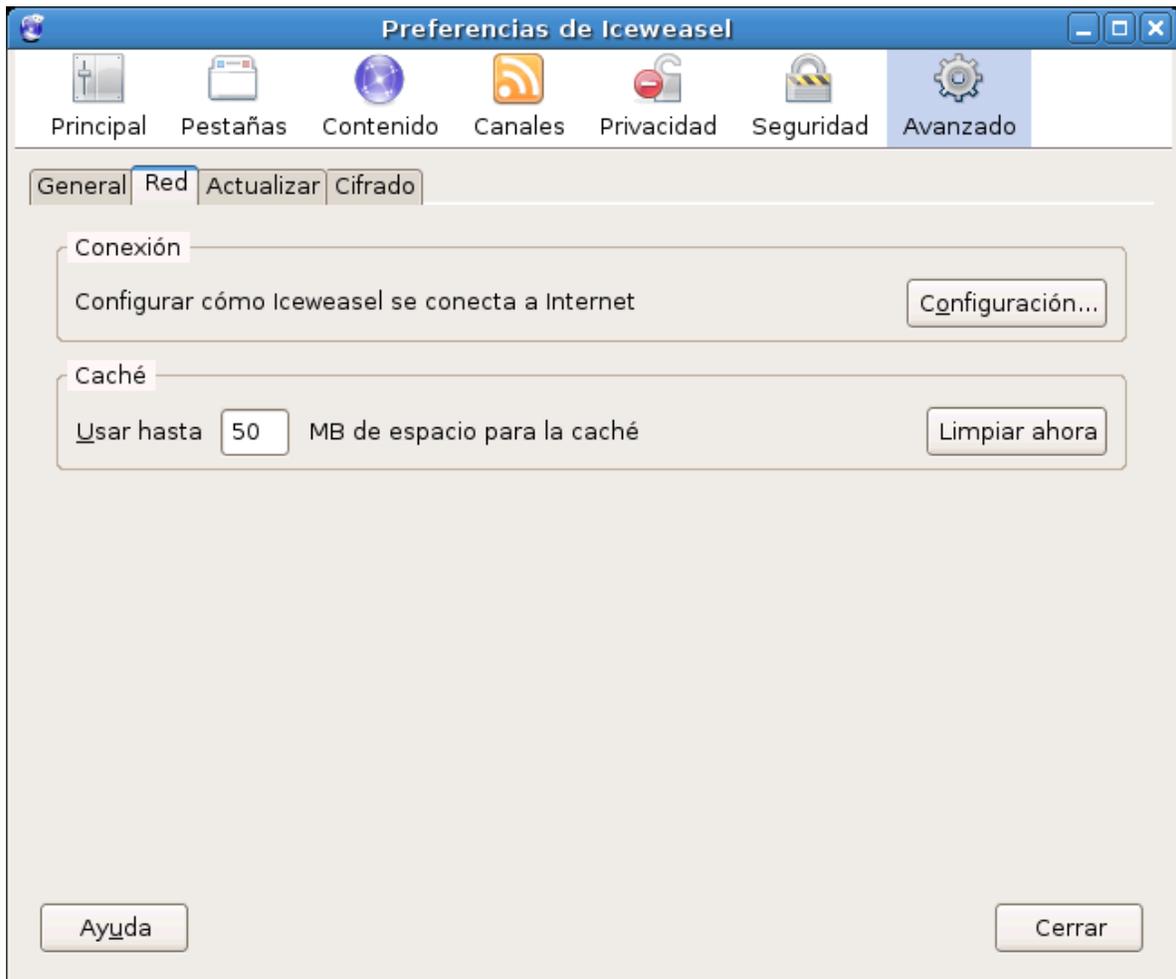
## [Imagen 85]



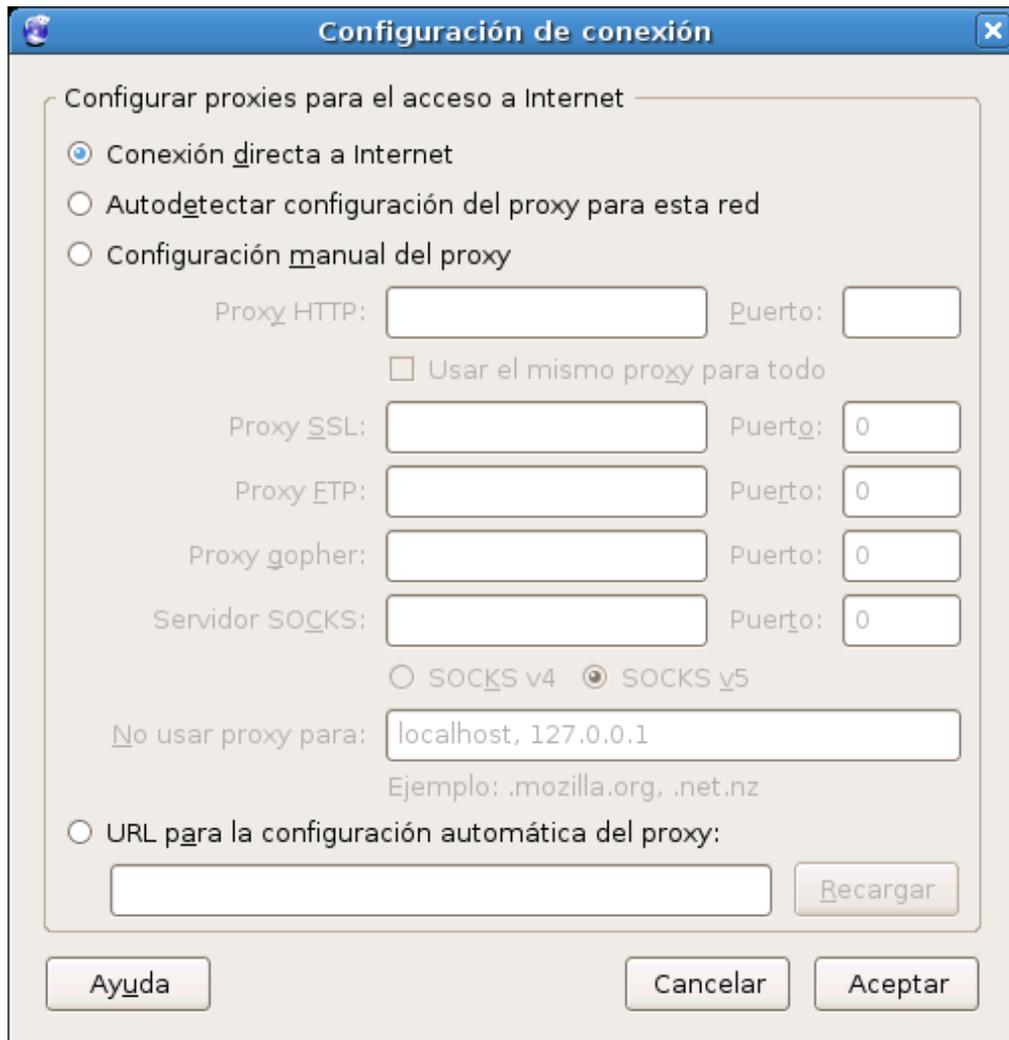
[Imagen 86]



[Imagen 87]



[Imagen 88]



[Imagen 89]

Configuración de conexión

Configurar proxies para el acceso a Internet

- Conexión directa a Internet
- Autodetectar configuración del proxy para esta red
- Configuración manual del proxy

Proxy HTT**P**:  Puerto:

Usar el mismo proxy para todo

Proxy SSL:  Puerto:

Proxy FTP:  Puerto:

Proxy gopher:  Puerto:

Servidor SOCK**S**:  Puerto:

SOCKS v4  SOCKS v5

No usar proxy para:

Ejemplo: .mozilla.org, .net.nz

URL para la configuración automática del proxy:

Recargar

Ayuda Cancelar Aceptar

**[Imagen 90]**

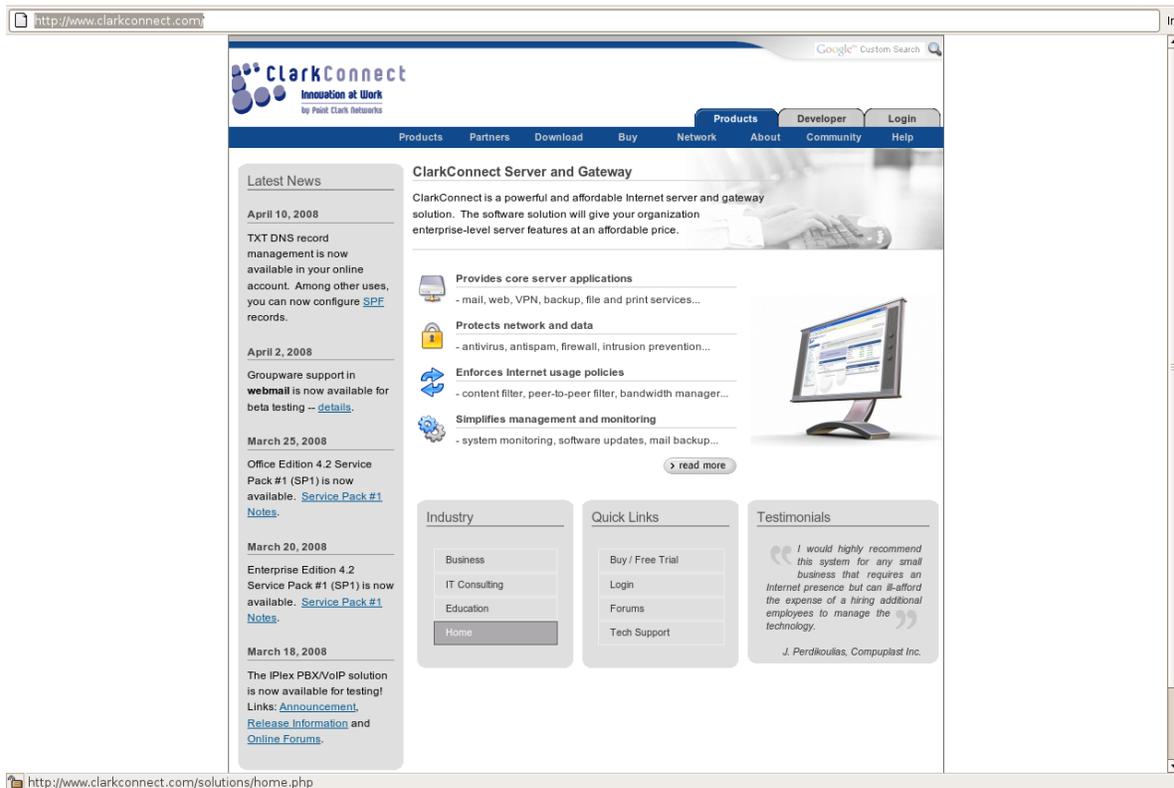


Dar clic en el *checkbox* Configuración manual del Proxy, se escribe la dirección de IP del ClarkConnect (192.168.1.254), seguido del puerto al cual se dirigen las conexiones. Por defecto el puerto 3128 es el designado si no se activó el filtro de contenido, de lo contrario el puerto sería 8080.

## 5.3.4 REGISTRAR EL SERVIDOR

Ahora, el paso siguiente es registrarse en la página oficial de *ClarkConnect* [www.clarkconnect.com](http://www.clarkconnect.com) .

[Imagen 91]

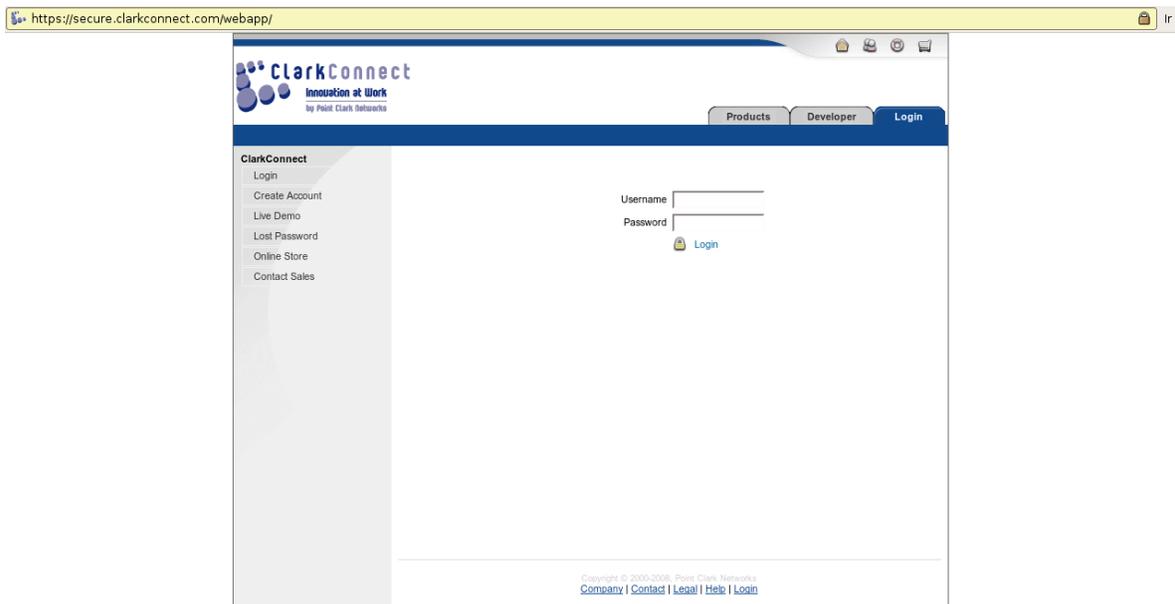


¿Por qué registrarse? Al registrarse se accede a una interfaz Web para administrar un sinnúmero de servidores diferentes, además de permitir al servidor descargar sus actualizaciones de *software* necesarias para el buen funcionamiento. Otro servicio que se obtiene es el de poder

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar  
asignarle al servidor una dirección, con un subdominio propio y un  
dominio de la compañía *ClarkConnect*; por ejemplo:

*ccsrv1.ppointclark.net*

[Imagen 92]



[Imagen 93]

**ClarkConnect**  
Innovation at Work  
by Point Clark Networks

Products Developer Login

**ClarkConnect**

- Login
- Create Account
- Live Demo
- Lost Password
- Online Store
- Contact Sales

**Create New Account**

By creating an account on this site, you **are not** obligated for any fees or charges. We keep your personal information private. To view our privacy policy in detail, [click here](#).

Thank you!

**Create New Account**

Username: Nombre

Password: \*\*\*\*\*

Password confirm: \*\*\*\*\*

E-mail: direccion\_de\_email@hostname

Country: Colombia

Timezone: GMT-05:00 (Etc/GMT+5)

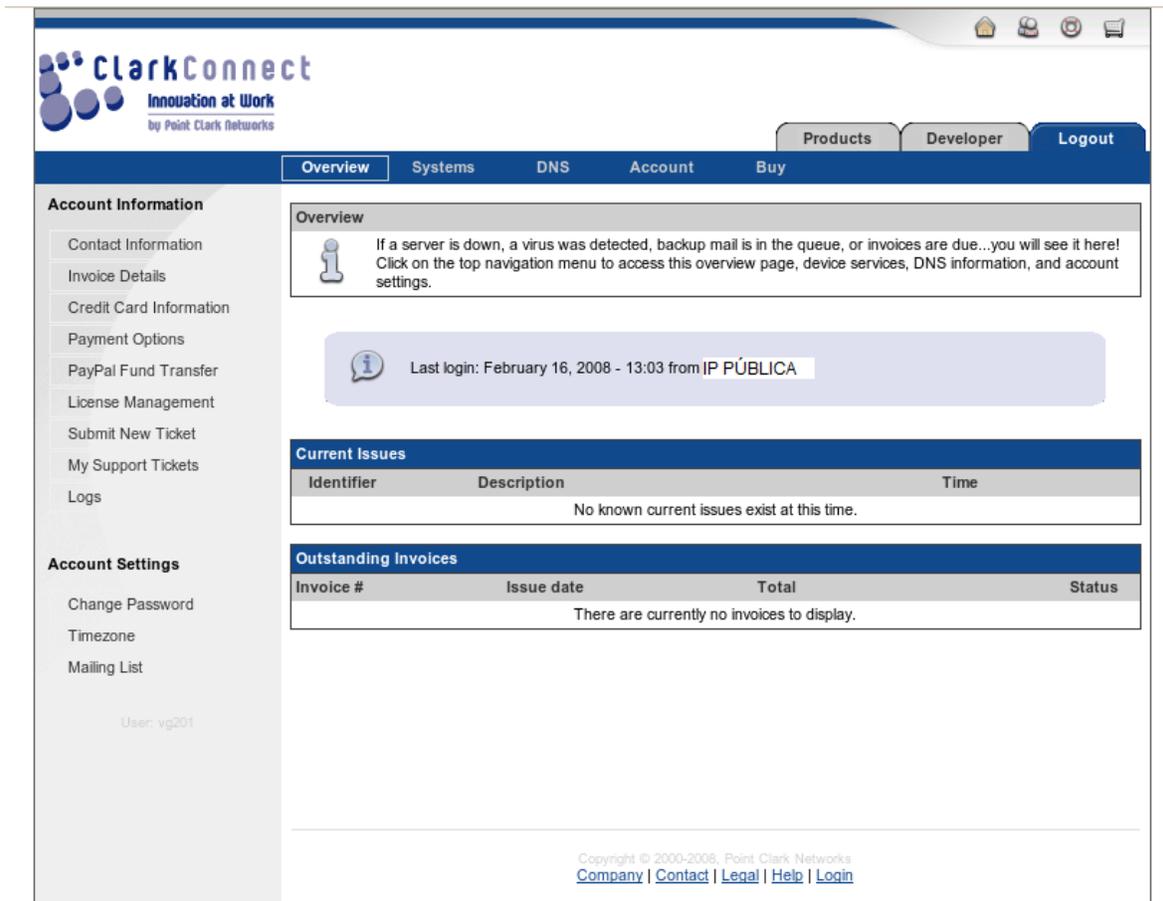
VAR ID: (Optional)

By clicking on "Create New Account" you accept the [Terms of Service](#).

[Create New Account](#)

Copyright © 2000-2008, Point Clark Networks  
[Company](#) | [Contact](#) | [Legal](#) | [Help](#) | [Login](#)

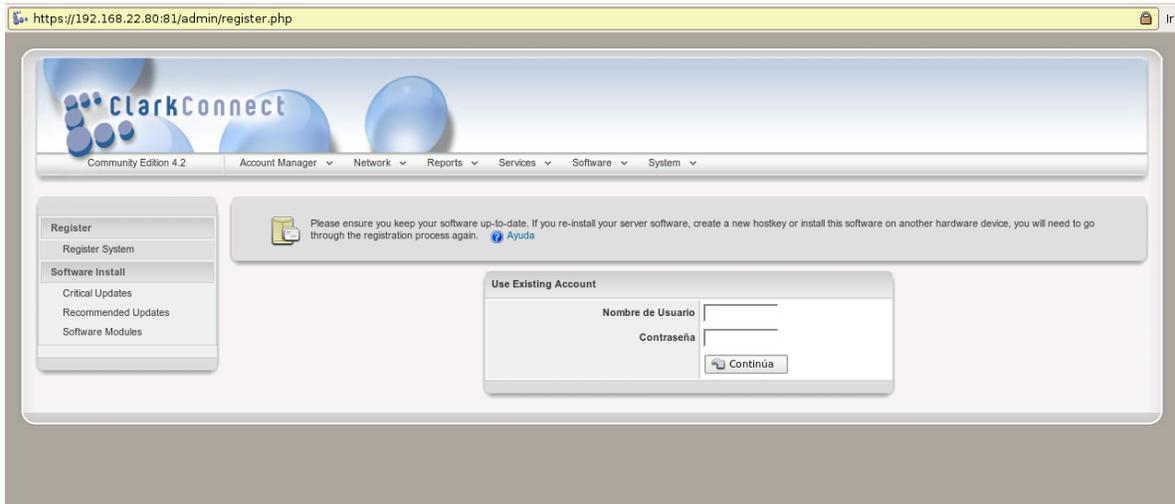
[Imagen 94]



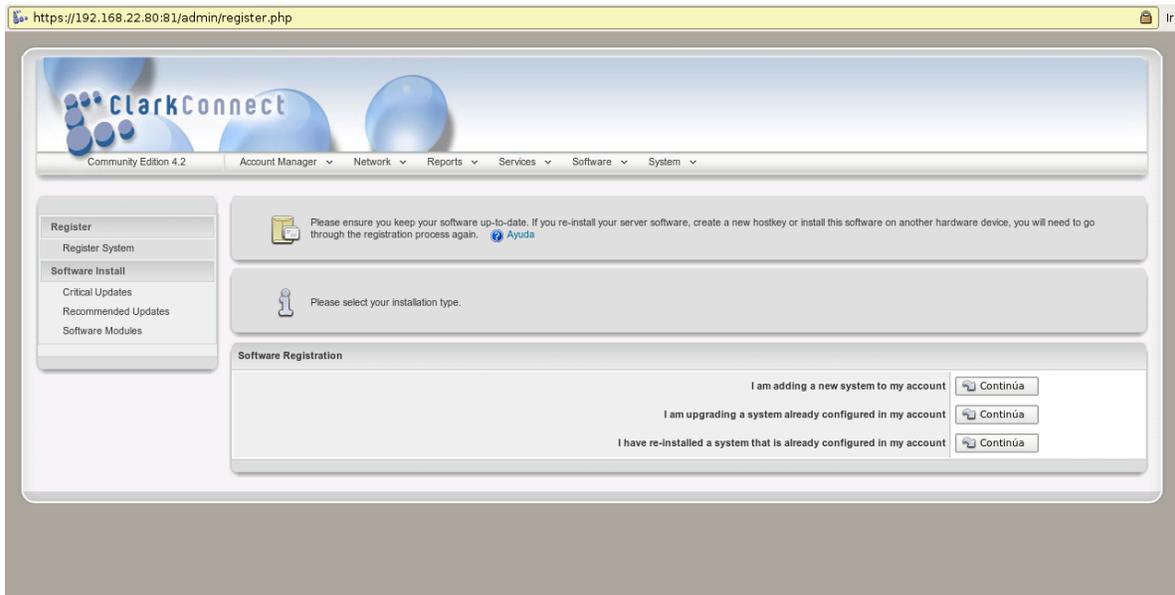
Luego de ingresar a la página y de obtener la cuenta, volvemos al servidor y nos dirigimos ahora a la sección Services>Register>Register System. Escribimos el nombre de usuario y la contraseña que usamos en la página de ClarkConnect. Esto nos lleva a una sección donde escogemos I am adding a new system to my account. A continuación escribimos el nombre del servidor, por ejemplo: *ccsrv1* , que significa:

# ClarkConnect **SerVidor 1**

[Imagen 95]

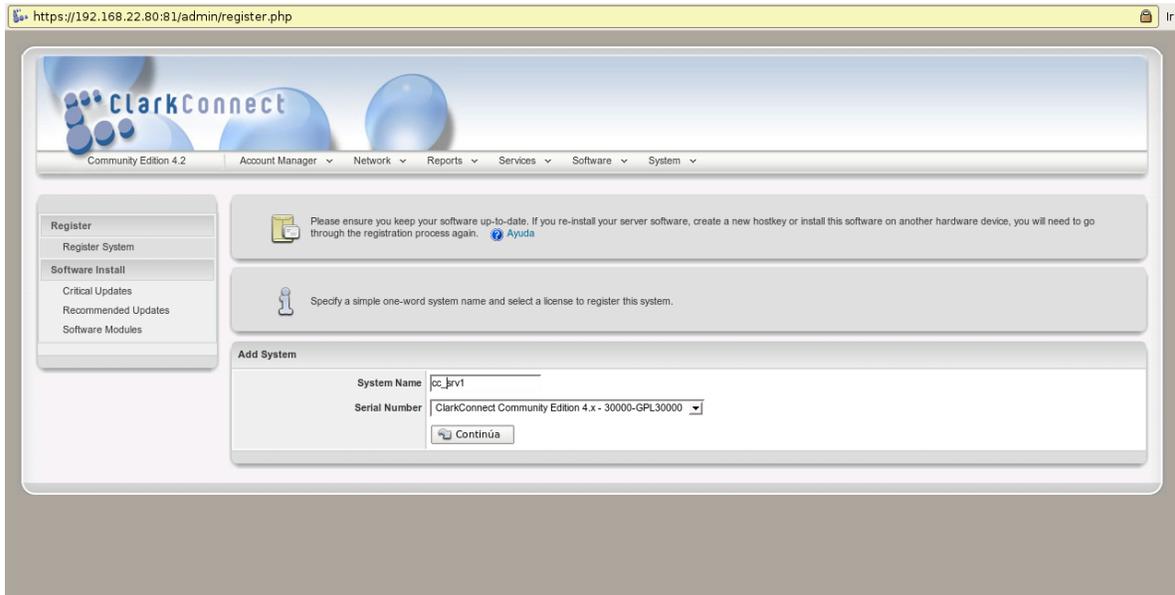


[Imagen 96]



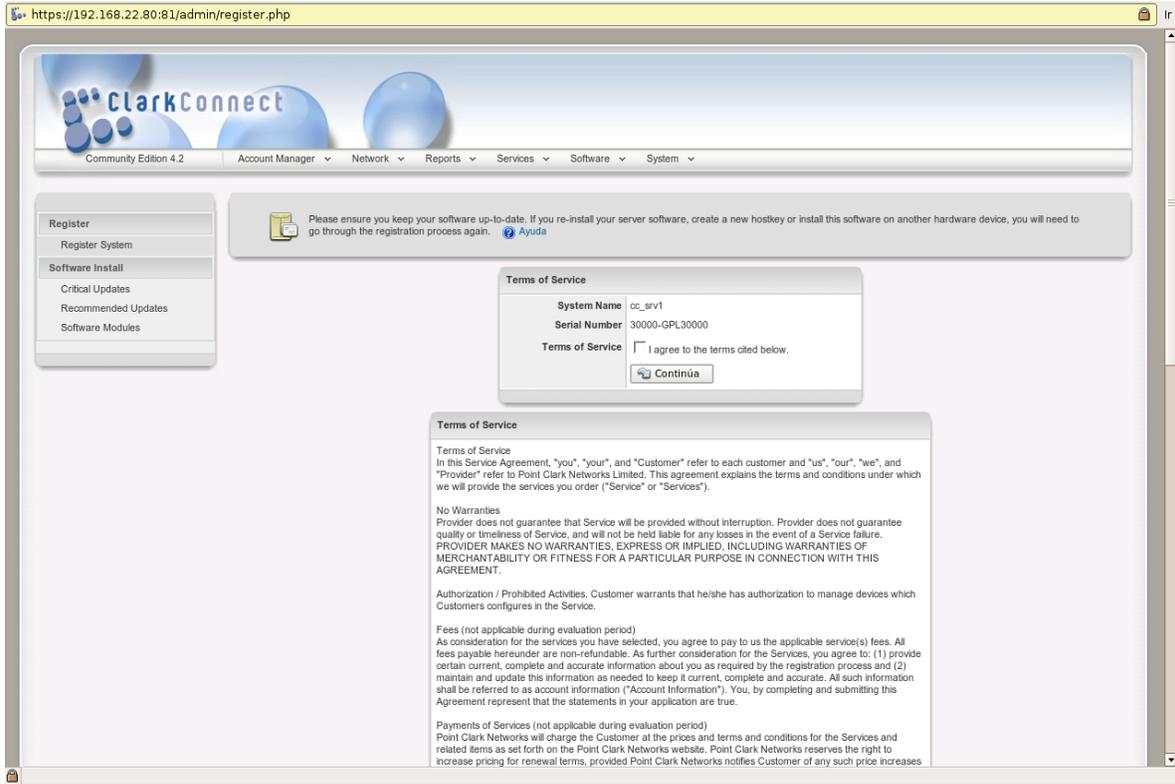
## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 97]



A continuación aceptamos la licencia, es recomendable leerla para tener una idea de nuestros derechos con respecto al *software* que acabamos de instalar. (Adjunto al texto se tiene una copia de las licencias que tiene el *ClarkConnect*.)

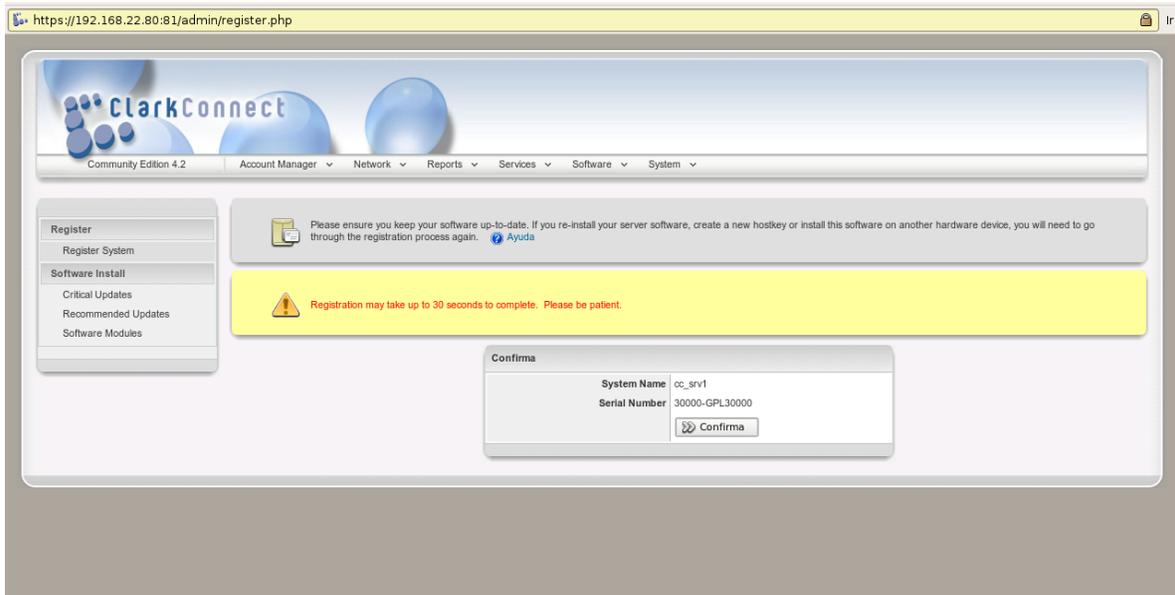
[Imagen 98]



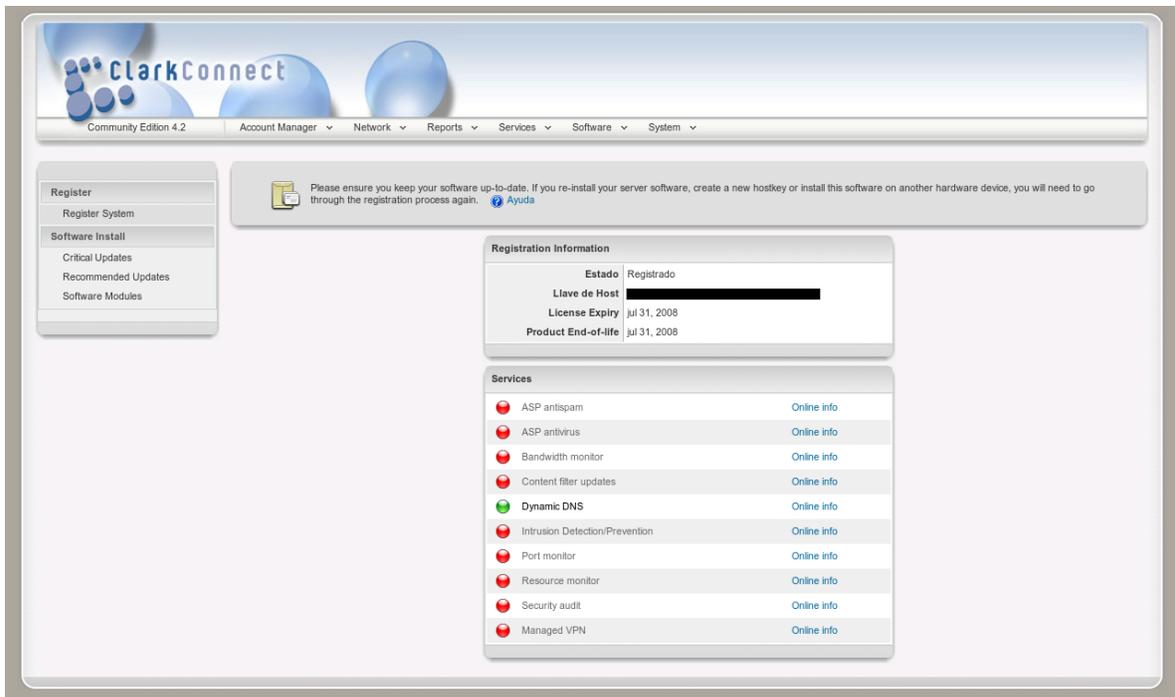
Y lo registramos. Transcurridos poco más de 30 segundos, presionamos continuar y nos lleva a una nueva página que nos muestra a qué servicios podemos acceder, y qué requisitos de información sobre nuestro equipo tenemos.

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 99]



[Imagen 100]



El único servicio que podemos usar de forma gratuita es el de *DNS* dinámico, esto nos facilita ubicar nuestro servidor en Internet evitando aprenderse la *IP* pública de éste siempre que cambie. Un ejemplo sería lo siguiente: Esta dirección apunta a nuestro servidor y cada vez que la ingresamos en un navegador podemos conectarnos remotamente al servidor (esto sólo se puede si se especifica hacerlo, mas información en los apartados siguientes). Esta dirección es otra forma de escribir la dirección de *IP* pública del servidor y que es más fácil de aprender.

200.111.80.222 --> ccsrv1.pointclark.net

Si revisamos en la página de *ClarkConnect*, podemos ver de ahora en adelante a nuestro servidor, con su respectiva dirección de *IP* pública, en la sección de *Systems*.

# Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen 101]

The screenshot displays the ClarkConnect web interface. At the top left is the logo for ClarkConnect, 'Innovation at Work by Point Clark Networks'. The navigation bar includes 'Overview', 'Systems' (selected), 'DNS', 'Account', and 'Buy'. On the right, there are buttons for 'Products', 'Developer', and 'Logout'. A left sidebar lists system management options for 'System: cc\_srv1', including 'System Information', 'Module Licenses', 'Weekly Report', 'System Logs', 'Alert Notify', 'Rename', and 'Delete'. Below this is a 'Services' section with various monitoring tools like 'ASP Antispam', 'ASP Antivirus', 'Bandwidth Monitor', 'Content Filter', 'Network/Dynamic DNS', 'Managed VPN', 'Intrusion Detection', 'Port Monitor', 'Resource Monitor', and 'Security Audit'. The main content area shows 'Dynamic DNS' is 'Enabled'. A configuration box contains: Subdomain 'ccsrv1', Domain 'pointclark.net', IP address 'IP PÚBLICA', and Last IP update 'Apr 11, 2008 - 13:43'. Below this is a 'Recent Activity' table:

Domain	IP	Update Type	Time
<input checked="" type="checkbox"/> ccsv1.pointclark.net	IP PÚBLICA	Manual IP update	Apr 11, 2008 - 13:45
<input checked="" type="checkbox"/> ccsv446.pointclark.net	IP PÚBLICA	Automatic IP update	Apr 11, 2008 - 13:43
<input checked="" type="checkbox"/> ccsv446.pointclark.net	IP PÚBLICA	Default dynamic DNS entry created	Apr 11, 2008 - 13:42

At the bottom, there is a copyright notice: 'Copyright © 2000-2008, Point Clark Networks' and links for 'Company', 'Contact', 'Legal', 'Help', and 'Login'.

[Imagen 102]

The screenshot shows the ClarkConnect web interface for managing DNS records. The header includes the ClarkConnect logo with the tagline "Innovation at Work by Point Clark Networks". Navigation tabs include Overview, Systems, DNS (selected), Account, and Buy. A secondary navigation bar contains Products, Developer, and Logout. The left sidebar lists DNS Records (A, CNAME, Mail/MX, TXT, Mail/MX Backup) and Domain/DNS Services (Domain Information, DNS/Domain Logs, Register Domain, Renew Domain, Transfer Domain, DNS Service, Renew DNS Service, Delete Domain). The main content area features a "DNS Summary" section with a globe icon and text explaining the DNS Information page. Below this is a table for "pointclark.net (Dynamic IP)" with two entries: "ccsrv1.pointclark.net" pointing to "IP PÚBLICA" and "servidortesis.pointclark.net" pointing to a redacted IP address. The footer contains copyright information and links for Company, Contact, Legal, Help, and Login.

ClarkConnect  
Innovation at Work  
by Point Clark Networks

Products Developer Logout

Overview Systems **DNS** Account Buy

**DNS Records**

- A Records
- CNAME Records
- Mail/MX Records
- TXT Records
- Mail/MX Backup

**Domain/DNS Services**

- Domain Information
- DNS/Domain Logs
- Register Domain
- Renew Domain
- Transfer Domain
- DNS Service
- Renew DNS Service
- Delete Domain

User: vg201

**DNS Summary**

The DNS Information page gives you all the tools to manage all of your DNS records, as well as register, renew and transfer domains. Not familiar with DNS? Here's a [DNS Primer](#).

**pointclark.net (Dynamic IP)**

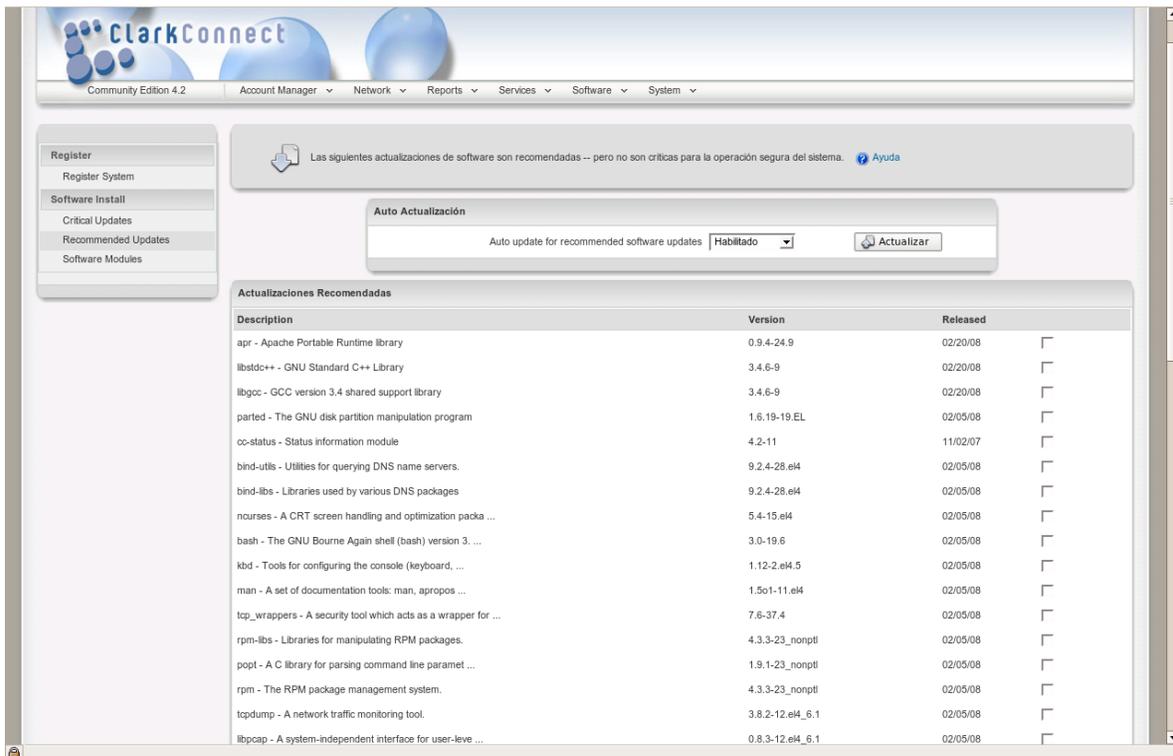
ccsrv1.pointclark.net	»»	IP PÚBLICA
servidortesis.pointclark.net	»»	[REDACTED]

Copyright © 2000-2008, Point Clark Networks  
[Company](#) | [Contact](#) | [Legal](#) | [Help](#) | [Login](#)

## 5.3.5 ACTUALIZAR E INSTALAR SOFTWARE ; ADMINISTRACIÓN REMOTA

Luego de registrar el sistema, necesitamos actualizar el *software* del servidor. Para hacerlo nos dirigimos a `Services>Recommended Updates`. Esto nos lleva a una sección que es recomendable revisar constantemente.

[Imagen 103]



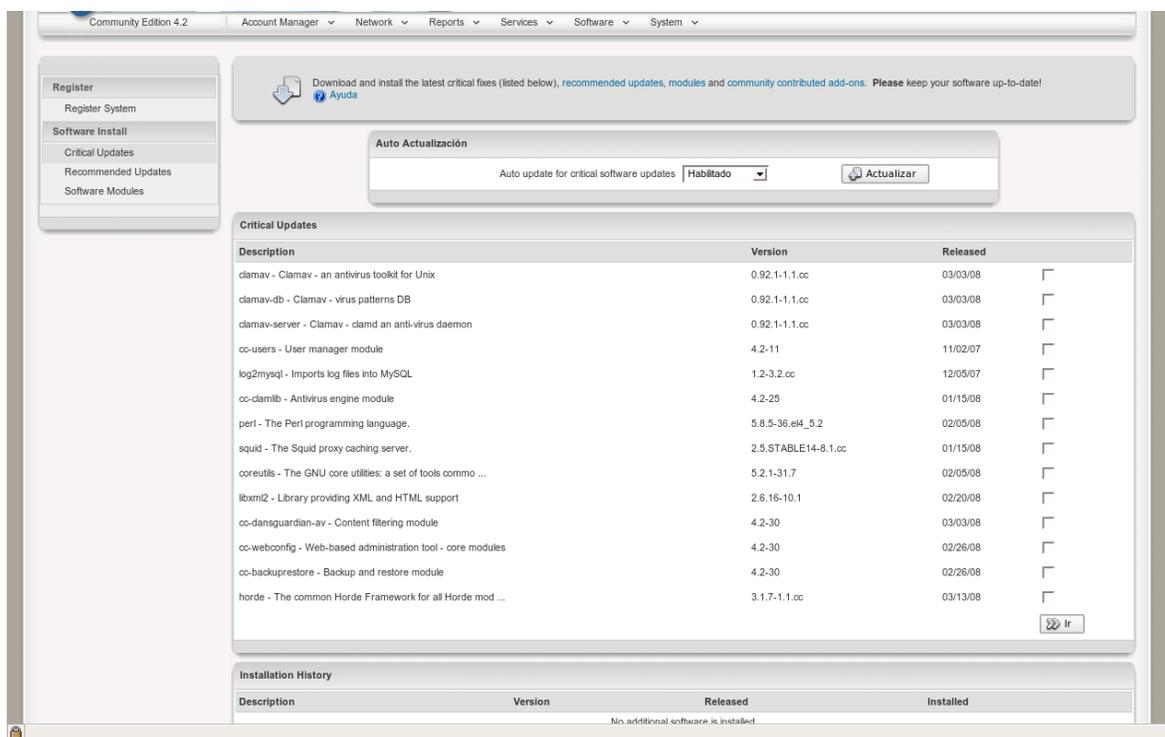
Las siguientes actualizaciones de software son recomendadas -- pero no son críticas para la operación segura del sistema. [Ayuda](#)

Auto Actualización  
Auto update for recommended software updates

Description	Version	Released	
apr - Apache Portable Runtime library	0.9.4-24.9	02/20/08	<input type="checkbox"/>
libstdc++ - GNU Standard C++ Library	3.4.6-9	02/20/08	<input type="checkbox"/>
libgcc - GCC version 3.4 shared support library	3.4.6-9	02/20/08	<input type="checkbox"/>
parted - The GNU disk partition manipulation program	1.6.19-19.EL	02/05/08	<input type="checkbox"/>
co-status - Status information module	4.2-11	11/02/07	<input type="checkbox"/>
bind-utils - Utilities for querying DNS name servers.	9.2.4-28.e4	02/05/08	<input type="checkbox"/>
bind-libs - Libraries used by various DNS packages	9.2.4-28.e4	02/05/08	<input type="checkbox"/>
ncurses - A CRT screen handling and optimization packa ...	5.4-15.e4	02/05/08	<input type="checkbox"/>
bash - The GNU Bourne Again shell (bash) version 3. ...	3.0-19.6	02/05/08	<input type="checkbox"/>
kbd - Tools for configuring the console (keyboard, ...	1.12-2.e4.5	02/05/08	<input type="checkbox"/>
man - A set of documentation tools: man, apropos ...	1.501-11.e4	02/05/08	<input type="checkbox"/>
tcp_wrappers - A security tool which acts as a wrapper for ...	7.6-37.4	02/05/08	<input type="checkbox"/>
rpm-libs - Libraries for manipulating RPM packages.	4.3.3-23_nonptl	02/05/08	<input type="checkbox"/>
popt - A C library for parsing command line paramet ...	1.9.1-23_nonptl	02/05/08	<input type="checkbox"/>
rpm - The RPM package management system.	4.3.3-23_nonptl	02/05/08	<input type="checkbox"/>
tcpdump - A network traffic monitoring tool.	3.8.2-12.e4_6.1	02/05/08	<input type="checkbox"/>
libcap - A system-independent interface for user-level ...	0.8.3-12.e4_6.1	02/05/08	<input type="checkbox"/>

La página nos muestra dos secciones cada una con listas, la primera con las actualizaciones que podemos realizar y la otra con el historial de las mismas. Para instalar debemos simplemente escoger qué *software* por medio de las casillas y presionar >>Go. Y continuamos siguiendo los mensajes que aparecen en pantalla. Después de unos minutos, de descargar e instalar el *software*, volvemos a la pantalla inicial de *Recommended Updates* para asegurarnos que todo haya quedado bien instalado.

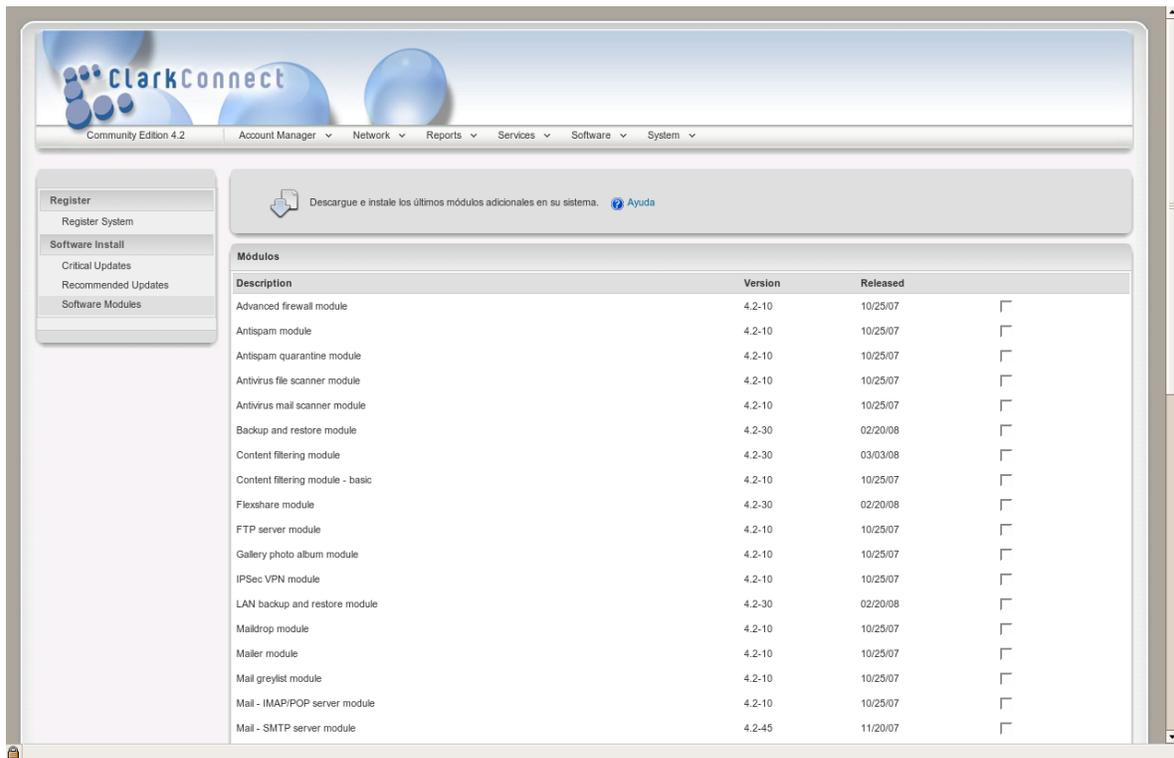
[Imagen 104]



Luego de realizar la actualización del *software*, pasamos a las actualizaciones críticas. Estas, como su nombre lo indica, son críticas

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar porque son correcciones a fallas de seguridad o parches para el *software* ya instalado. Los pasos para agregar estos parches y correcciones son iguales que los descritos anteriormente.

[Imagen 105]



Finalmente una parte importante y que posibilita expandir las capacidades y posibilidades de el servidor: la instalación de módulos de *software*. Estos mismos módulos son los que podíamos escoger durante la instalación. Varios de los módulos pueden servir para un mismo servicio pero manejar diferentes tareas, por ejemplo: podemos tener nuestro propio servidor de correo electrónico, instalando los módulos *Mail - SMTP* (protocolo de envío), *Mail - IMAP/POP* (protocolos para

recoger el correo) y *Mailer module* (el programa para mandar el correo) .

Lo que describí arriba es uno de los dos métodos para actualizar e instalar *software* en un servidor *ClarkConnect*. El segundo requiere estar frente al servidor (con teclado y pantalla). Para ello realizamos los siguientes pasos:

Cuando el servidor es encendido y carga completamente nos muestra un fondo negro con una ventana roja preguntando por la contraseña del superusuario o *root*,

1. Abrir consola: presionamos `Alt + F2` (se puede tener hasta 5 consolas presionando de la tecla `F2` a la `F6`).
2. Ingresamos el nombre del superusuario: `root`
3. Escribimos su contraseña.
4. Y nos encontramos con: `[root@ClarkConnect ~]#`. Esto significa que el intérprete de órdenes o *shell* esta esperando nuestros comandos para ejecutarlos.
5. Escribimos `apt-get update` ; este comando actualiza las bases de datos de *software*. (*Apt-get* es un eficiente programa para el manejo de paquetes de *software* y conviene aprender a usarlo, para esto basta con ejecutar `man apt-get` lo cual nos mostrará un resumen del programa y sus funciones para poder usarlo). *Apt-get* se conectará a Internet, más específicamente a los servidores de `clarkconnect.com`, donde sincroniza las fuentes de *software* con las descargadas.

6. Ahora ejecutar `apt-get upgrade` ; como lo indica el comando lo que se hace es instalar las versiones más nuevas de todo el *software* instalado en el equipo. Es posible que en esta etapa `apt-get` pregunte si desea instalar el *software* seleccionado, se presiona 'Y' seguido de la tecla *Enter* y continuamos con la instalación. Todo este proceso es automático, la interacción con el usuario es mínima.

En este momento si finalizó correctamente la instalación del *software* aparece nuevamente la *shell* pidiéndonos un nuevo comando para introducir. El siguiente paso es opcional, pero es recomendable ejecutarlo periódicamente.

7. En el intérprete de órdenes escribimos `apt-get dist-upgrade` y realiza pasos similares al punto 6. Con este comando le decimos al `apt-get` que busque el *software* disponible y lo actualice de forma inteligente a una versión mas nueva. Este paso se realiza para pasar de la versión del *ClarkConnect* 4.2 a las 4.3 por ejemplo.

Para salir de la consola basta con escribir `exit` o presionar `Ctrl + D` .

Existe una forma para conectarse remotamente al Servidor/Firewall desde cualquier computador en la red y usar una consola como si se estuviera presente, este método se considera poco seguro, dado que se deja un puerto abierto en el servidor todo el tiempo. Aun así las ventajas

que traen son varias y consideramos que podemos correr el riesgo.

*SSH (Secure Shell)* es el nombre de un protocolo y del programa que lo implementa. *SSH* sirve para conectarse remotamente a máquinas en una red y permite manejar y manipular la máquina mediante una consola. Adicionalmente, posee la ventaja de entablar una conexión de forma segura y cifrada, así que toda la información que se envíe desde los dos nodos se encuentra protegida.

Para habilitar este servicio en una cuenta de usuario, se ingresa a una consola como superusuario.

Creamos un nuevo usuario, con este accederemos al equipo, por razones de seguridad no usaremos el *root* o superusuario, pero si algunos trucos para tener sus privilegios sin vulnerar mucho al servidor. Ejecutamos en la consola como *root* (sólo como superusuario podemos crear, eliminar o modificar usuarios).

1. [root@ClarkConnect ~]# *useradd [nombre\_de\_usuario]*

Con este comando creamos un nuevo usuario .

2. [root@ClarkConnect ~]# *passwd [nombre\_de\_usuario]*

Aquí indicamos que le queremos modificar la contraseña al usuario especificado. Leer nuevamente el apartado 4.5.1, la sección donde se muestra cómo crear la contraseña de *root*.

Se recomienda tener una palabra clave diferente para esta cuenta, pero que aun así las dos contraseñas sean seguras.

Basta recordar, en lo posible evitar escribir las contraseñas en lugares de fácil acceso como un cuaderno. En lo preferible

**no escribir nunca las contraseñas.**

3. [root@ClarkConnect ~]# *usermod -s /bin/bash*

*[nombre\_de\_usuario]*

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

Este comando permite que el usuario pueda entrar a la máquina remotamente por medio de *SSH*.

Como mencioné anteriormente se puede ingresar remotamente al servidor por medio del protocolo *SSH*. Existen dos alternativas, una para cada SO. En *Windows* necesitamos del programa llamado *PuTTY*, lo podemos descargar desde [www.putty.org](http://www.putty.org) o en su versión portable que no necesita instalación en:

[http://portableapps.com/apps/Internet/putty\\_portable](http://portableapps.com/apps/Internet/putty_portable)

El ejecutarlo nos muestra una ventana donde introducimos la *IP* o Dirección del *host*, el servidor *ClarkConnect*, presionamos conectar y una consola se abre preguntando por el usuario y la contraseña. Escribimos el usuario que creamos anteriormente y su respectiva contraseña. Ahora con este nuevo usuario podemos ingresar remotamente al servidor y si necesitamos realizar tareas administrativas, para cambiar al usuario *root* ejecutamos: *su -*

Al presionar *Enter* preguntará por la contraseña del superusuario. Si realizamos todo bien, nos encontraremos ahora con los máximos privilegios para realizar las tareas administrativas. Otra forma de obtener privilegios *root* sin ingresar a una sesión de superusuario es ejecutar los comandos que requieran permisos de *root* de esta forma:

```
sudo [comando_a_ejecutar_con_sus_opciones]
```

Ejemplo: `sudo ifconfig eth1`

Estos comandos mostrarán la información de la interfaz de red *eth1*.

El comando `sudo` es un comando que nos permite ejecutar los comandos siguientes a él con permisos de *root*, pero sólo si conocemos la contraseña de lo contrario no se podrá.

Desde una terminal con *GNU/Linux* para ingresar al servidor remotamente ejecutamos en consola el siguiente comando:

```
ssh -p 22 [nombre_de_usuario]@[dirección_del_servidor]
```

Ejemplo: `ssh -p 22 rsh@192.168.0.254` . Lo que este comando hace es ejecutar el comando `ssh` conectándose al servidor con la *IP* 192.168.0.254 (aquí la *IP* puede variar, puede ser tanto una dirección numérica como un nombre de dominio *clarkconnect.lan*) a través del puerto 22 como el usuario `rsh`.

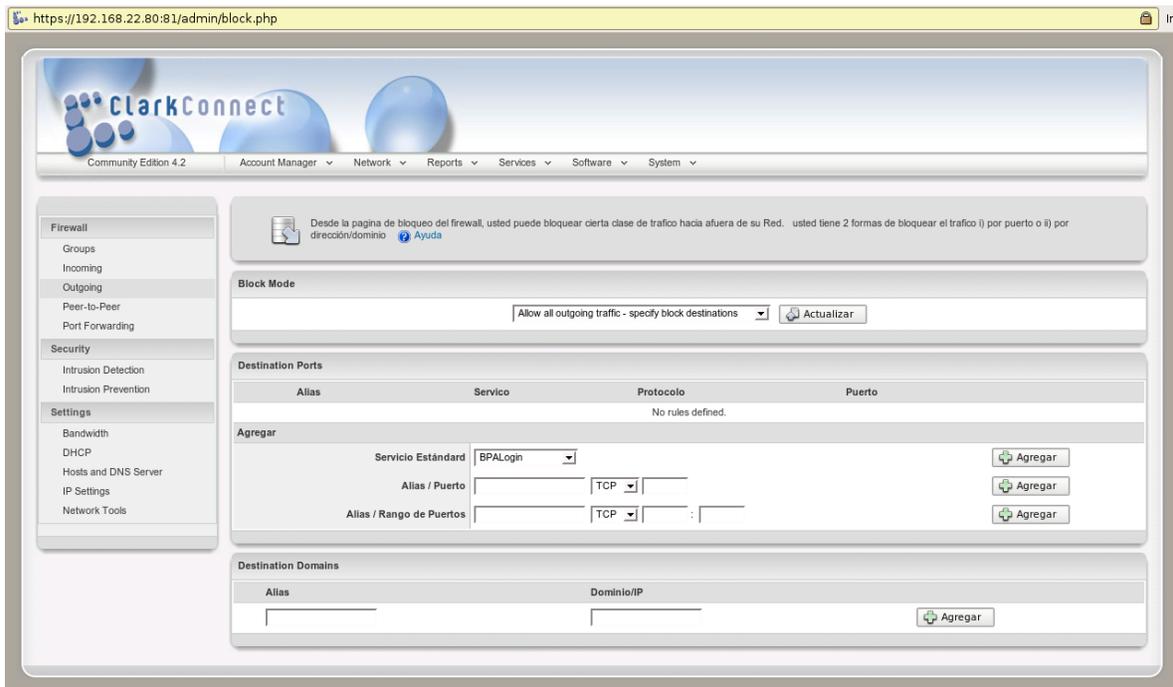
## **5.3.6 CONFIGURACIÓN DEL FIREWALL**

Llegamos a una de las secciones mas importantes en todo este trabajo escrito. Aquí examinaremos, configuraremos y probaremos las opciones que nos brinda el *Firewall* del *ClarkConnect*. Para este momento ya debemos saber que es y para que sirve un *Firewall*, si este no es el caso por favor leer las secciones 3.1 y 3.2.

### **5.3.6.1 OUTGOING (SALIDA)**

Desde el *Webconfig* nos dirigimos a *Network --> Outgoing*. En esta sección se podrán bloquear o permitir ciertos tipos de tráfico que salen de la red, como por ejemplo programas de mensajería instantánea (*MSN Messenger*), descargas ilegales de musica por medio de programas *P2P* y mucho mas.

[Imagen net1]



Para seleccionar una de las dos opciones (bloquear o permitir) se seleccionada el modo de bloqueo (*Block Mode*). Las dos opciones presentes son muy útiles dependiendo del uso que se le dará al servidor. Por defecto el modo para bloquear todo el tráfico de salida se encuentra activado (*Block all outgoing traffic*), lo que se hace para evadir este modo es especificar los distintos servicios, protocolos, destinos y puertos a los que se les permitirá salir. De forma opuesta funciona el otro modo de bloqueo (*Allow all outgoing traffic*), este permite todo el tráfico de salida a excepción de los servicios, protocolos, destinos o puertos que se especifiquen. Para nuestro caso, implementar el *Firewall* en un entorno escolar, escogemos *Block all outgoing traffic*, de esta forma se podrá impedir el acceso a Internet de todo el *software* que no exista en

la lista blanca que vamos a crear a continuación.

En medio de la página se muestran los puertos de destino que han de ser bloqueados o permisos según sea al caso. Las esferas rojas o verdes muestran el estado de la regla, roja para deshabilitada y verde para activada. Seguido se muestra el nombre de la regla, este puede ser cualquier texto alfanumérico, lo aconsejable es describir de una forma corta, sencilla y entendible que función tiene la regla. Continuando se ve el nombre original del servicio, el protocolo que emplea *TCP* (para conexiones en las cuales se transmiten datos, garantizando que estos se entreguen correctamente en el destino) y *UDP* (para la transmisión de datos sin realizar conexiones con el destino); el puerto por el cual se bloquea o se permite el flujo de datos de salida. Las dos opciones finales permiten borrar (*Delete*) la regla, habilitarla (*Enable*) o deshabilitarla (*Disable*) según sea el caso. Esta información es la que hay que tener en cuenta cuando se tengan problemas para llegar a Internet con algún programa o servicio.

En la sección *Add* añadimos las reglas que se necesiten. Tiene dos principios sencillos:

1. Especificar un servicio, nombre de la regla y puerto o rango de puertos;
2. Añadir una regla según la lista del menú desplegable.

La última sección *Destination Domains* funciona de forma similar solo que en este caso se escribe el dominio o dirección de *IP* que se desee añadir. En *Standard Services* se puede seleccionar de la lista un objeto, este describe un servicio para bloquear o permitir; pero si el servicio,

programa o protocolo no existe en la lista, se usa el formato siguiente, donde se especifica un nombre o sobrenombre, el protocolo de transmisión (*TCP/UDP* son los principales, los otros son para conexiones *VPN*) y finalmente el puerto o un rango de puertos.

Seleccionado el modo `Block all outgoing traffic` se añaden los siguientes servicios necesarios para navegar cómodamente y que se desean que salgan a Internet:

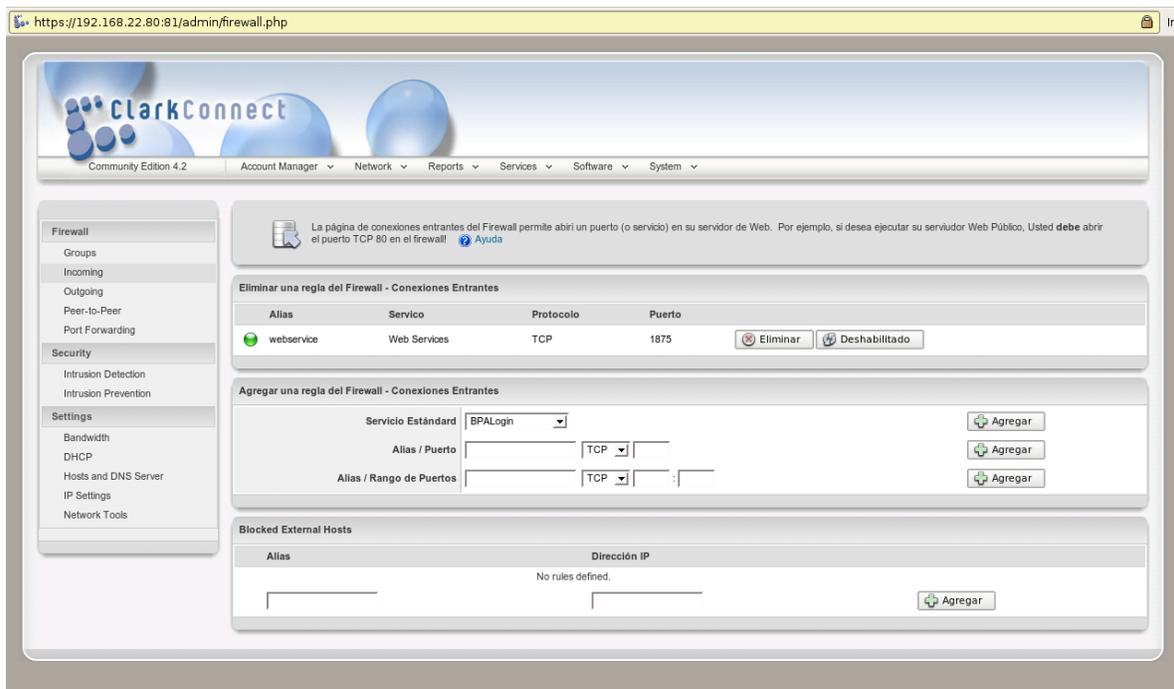
1. *HTTP* y *HTTPS* - Navegar por la páginas de Internet (*Internet Explorer, Mozilla Firefox*)
2. *IMAP* e *IMAPS* - Protocolo para la transmisión de correo (*MS Outlook, Thunderbird*)
3. *POP3* y *POP3S* -- Protocolo para la transmisión de correo (*MS Outlook, Thunderbird*)
4. *SMTP* -- Protocolo para la transmisión de correo (*MS Outlook, Thunderbird*)

Servicios opcionales y/o útiles:

5. *FTP* - Protocolo para la transferencia de archivos
6. *PassiveFTP* -- Protocolo para la transferencia de archivos
7. *ICQ/AIM* - Servicio de mensajería instantánea (*ICQ*)
8. *MSN* -- Servicio de mensajería instantánea (**MSN Messenger**)
9. *NTP* - Servicio para sincronizar por internet los relojes de los computadores

### 5.3.6.2 INCOMING (ENTRADA)

[Imagen net2]



En esta sección del *Firewall* se especifican que servicios, puertos, protocolos y dominios que pueden ingresar al servidor o la *LAN* sin ser bloqueados por el *Firewall*. Esta sección es útil por ejemplo: si se tiene un servidor Web y se desea que sea visitado desde el Internet.

Esta sección funciona de forma muy similar a la anterior *Outgoing*. Se tiene una lista de las reglas, las cuales están habilitadas o deshabilitadas; y un formato para añadir nuevas. De igual forma se borran y se agregan los servicios, protocolos y puertos según sea la

necesidad.

Aunque el servidor se encuentra recién instalado, se ve que ya existe una regla llamada *Webservice*. Esta permite el ingreso de conexiones TCP por el puerto 1875 el cual es usado por los servidores de `pointclark.net` para conocer el estado de nuestro servidor además de otra información útil para la administración remota del servidor como: la dirección de IP Pública, el nombre y el estado del servidor entre otros. Si se contratan servicios (como control de ancho de banda, monitor de seguridad, etc; sección *Register System*) de *Point Clark Networks* estos usarán este servicio para conectarse a Internet. Para mayor información remitirse a: <http://www.ClarkConnect.com/info/suva.php>

Lista de los servicios para agregar a las reglas de *Incoming*:

1. *Webservice* - Control del servidor desde `pointclark.net`
2. *SSH - Secure Shell* para administración remota
3. *Webconfig* - Interfaz Web para administración remota

Estos servicios habilitados nos permitirán administrar el servidor *ClarkConnect* desde cualquier lugar del mundo con acceso a Internet. Por cuestiones de seguridad evitar conectarse con el servidor desde un lugar público como un café Internet o similar; al servidor solo se debe acceder con un computador del cual se sabe que es seguro. Evitar en su mayor parte usar el superusuario o *root* para evitar posibles infiltraciones por robo de contraseñas.

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

Si se desea tener un servidor de correo (*mail server*) o un servidor Web, se deben abrir los puertos a través de los servicios de la lista, ejemplo:

1. *HTTP* y *HTTPS* - Protocolos de transferencia de hipertexto  
(Servidor Web)
2. *IMAP* e *IMAPS* - Protocolos para transferencia de correo  
(Servidor Correo)
3. *POP3* y *POP3S* - Protocolos para transferencia de correo  
(Servidor Correo)
4. *SSH* - Protocolo para transferencia de correo (Servidor Correo)
5. *Webmail* - Acceso a la interfaz Web para el correo remoto

Si se desea permitir el acceso a la red local a una dirección de *IP* o un dominio específicos se debe escribir en la ultima sección para así permitir el ingreso.

## 5.3.6.4 PORT FORWARDING (REENVÍO DE PUERTOS)

[Imagen net3]

The screenshot shows the ClarkConnect web interface for port forwarding configuration. The browser address bar displays `https://192.168.22.80:81/admin/portfw.php`. The interface includes a navigation menu on the left with categories like Firewall, Security, and Settings. The main content area features a header with the ClarkConnect logo and a navigation bar. Below this, there is a descriptive text box and a table for configuring port forwarding rules. The table has columns for Alias, Service, Protocol, From Port, To Port, and A IP. Three rule templates are visible, each with an 'Agregar' button.

Alias	Servicio	Protocolo	Desde Puerto	Al Puerto	A IP
	BPALogin				
	TCP				
	TCP	Rango de Puertos			

El reenvío de puertos se usa para conectarse a una máquina dentro de una LAN cuando se encuentra en Internet. Ejemplo: se está en la casa y se desea revisar una máquina dentro de una LAN, normalmente acceder a esa máquina es difícil si el Firewall que la protege no tiene configurado una regla de reenvío de puertos. Sabemos que la máquina corre un servicio de SSH por el puerto 2222, como el servidor ClarkConnect ya usa el puerto 22 se debe especificar uno nuevo; se configura una regla en el Firewall para que cada vez que reciba una petición de conexión al

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

puerto 2222 reenvíe esa petición a la máquina a la cual deseamos conectarnos. Es simple en realidad. Y se puede aplicar para casi cualquier protocolo y tipo de conexión que se necesite. Y no solo para acceder a la red local desde Internet sino también a la inversa, conectarse desde la *LAN* a otra máquina en Internet.

Igual que en las secciones anteriores (*Outgoing* e *Incoming*) funciona la administración de las reglas de reenvío de puertos (*port forwarding*).

Si se desea añadir un servicio esta vez es necesario especificar un nombre para la regla, es de mucha ayuda especificar un nombre que explique a que máquina redirige que servicio o puerto, ejemplo:

```
SSH_maq1 TCP 2222 --> 2222 192.168.1.10
```

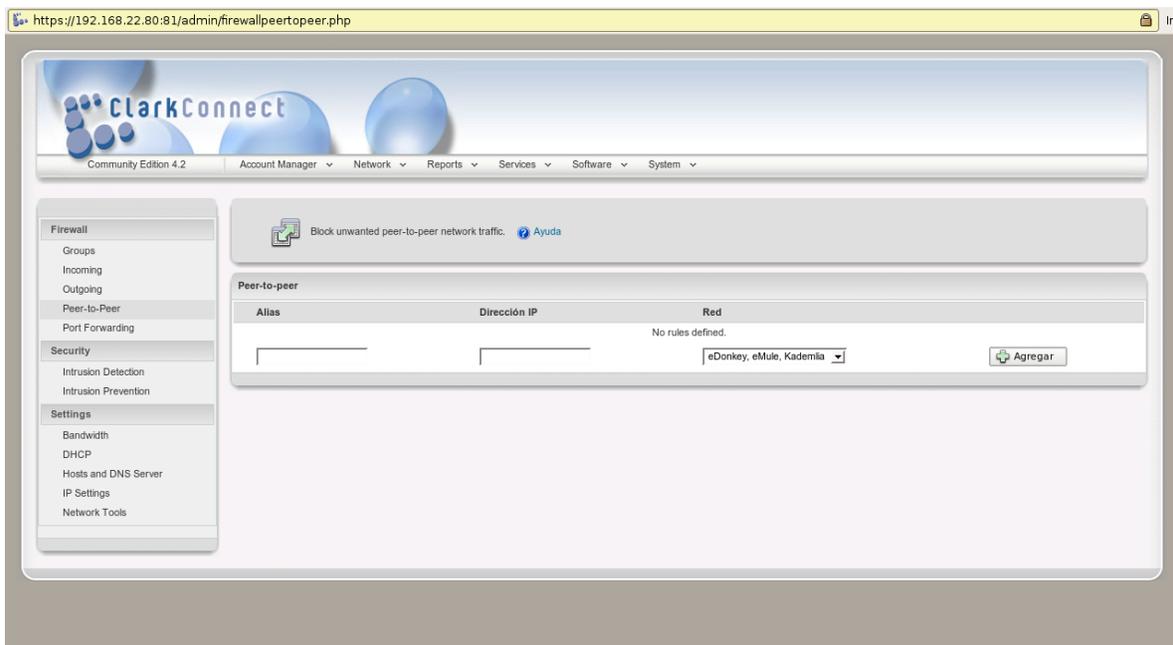
Esta regla llamada *SSH\_maq1*, que significa servicio de *SSH* en la máquina 1, redirige el intento de conexión por el puerto 2222 a la máquina con *IP* 192.168.1.10 .

De la misma forma que se crearon reglas personalizadas en los apartados anteriores se realiza en esta sección.

En este momento no es necesario la creación de ninguna regla para el reenvío de puertos, así que podemos continuar con el siguiente apartado.

### 5.3.6.5 PEER-TO-PEER (P2P)

[Imagen net4]



En esta sección del *Firewall* se bloquea el uso del *software P2P (Peer-to-Peer)*, por el cual se comparten archivos, los cuales pueden contener contenido protegido por derechos de autor o cualquier otro tipo de contenido que pueda ser peligroso para un menor de edad, como pornografía u otro tipo de contenido violento.

Desde la interfaz Web, escogeremos un nombre para la regla de bloqueo, seguido de una dirección de *IP*, si este espacio se deja en blanco se bloquearán todas las redes a las cuales tiene acceso el

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

*Firewall*, finalmente se escoge el protocolo *P2P* o el nombre del programa.

Esta sección funciona de forma similar a la anteriores en cuanto a añadir, habilitar o borrar reglas (de bloqueo).

### **5.3.6.6 ADVANCED -- CREAR REGLAS AVANZADAS**

Esta sección es una herramienta que se puede usar para crear reglas mas especiales para el *Firewall*. Como por ejemplo: permitir la conexión para administrar remotamente el servidor por medio del *Webconfig* pero solo para una única dirección de *IP*.

Al ingresar a esta sección vemos la lista de reglas que se han creado, si el servidor es una instalación fresca (nueva) esta sección estará vacía.

Para agregar una nueva regla se selecciona el tipo:

- *Incoming Allow*, Permitir de llegada
- *Incoming Block*, Bloquear de llegada
- *Outgoing Block*, Bloquear de salida
- *Port Forward*, Reenvío de puertos

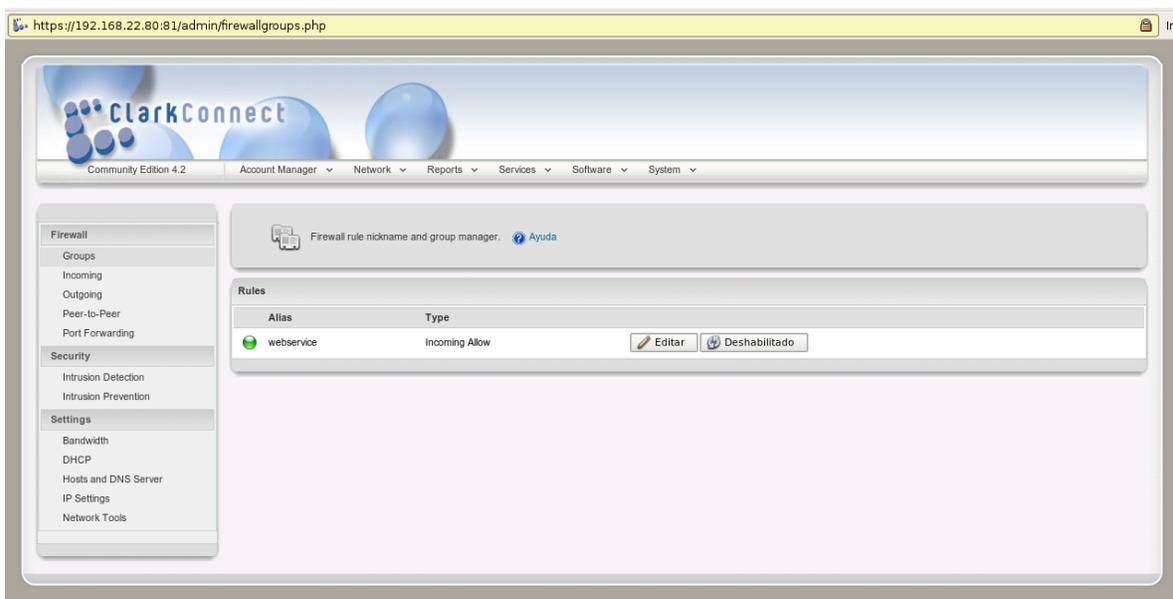
Terminado esto se presiona *Add* y llegamos a una ventana donde

podemos crear la nueva regla. Todas las ventanas son iguales, lo único que cambia entre ellas es el tipo de regla escogido anteriormente.

Se le da un nombre a la regla, se selecciona un grupo, si no existe se puede crear escribiéndolo en el espacio en blanco, en el apartado siguiente (5.3.6.7) se tratarán mas a fondo los grupos de reglas. Se selecciona el protocolo (*AH, ESP, GRE, IP TCP* ó *UDP*), los dos últimos son los protocolos mas comunes para las tareas de este servidor, los otros se refieren a protocolos de telefonía *IP* o para *VPN*. A continuación se puede especificar una dirección fuente de *IP* o *MAC (Source Adress)*, esta es la dirección de donde proviene la petición, por ejemplo: la dirección *IP* de la única máquina local que puede acceder al servidor por medio de *SSH*. Si no se especifica serán todas las direcciones de la red. Seguido se el puerto o el rango de puertos (*Source Port*) que se requiere. De la misma forma funcionan las direcciones y los destinatarios (*Destination Adress/Port*). Finalmente se presiona *Add* para crear la regla o *Cancel* para borrarla y crear una nueva.

### 5.3.6.7 FIREWALL GROUP MANAGER (ADMINISTRADOR DE GRUPOS)

[Imagen net5]



El administrador de grupos es una utilidad que permite organizar todas las reglas del *Firewall* de forma que sea fácil apreciar a que grupo pertenecen. Las reglas que no pertenezcan a un grupo específico se muestran al inicio de la página, conforme se baja se muestran los grupos creados que albergan a las otras reglas. Para cambiar una regla se presiona en *Edit*, para habilitarla o deshabilitarla se presiona el botón correspondiente. Para saber si una regla se encuentra activada o desactivada se debe mirar el color de la esfera a la izquierda del nombre

de la regla. Si se presiona editar nos lleva a una ventana donde podemos ver como se encuentra la regla configurada, a su vez podemos cambiar el nombre (*nickname*) y asociarla a un grupo existente por medio de la lista desplegable, si el grupo no existe se crea uno nuevo escribiendo el nombre en la casilla vacía junto a la lista.

El administrador de grupos posibilita desactivar, activar o borrar un conjunto de reglas facilitándole la labor al administrador de la red. Para esto es necesario bajar al final de la página, allí se muestra los nombres de los grupos existentes creados por el usuario y junto a los nombres las acciones que se pueden realizar.

En este momento el *Servidor/Firewall* se debe de encontrar completamente funcional es recomendable realizar un *backup* de la configuración actual, para ello se recomienda saltar a la sección 5.3.11.2 y luego continuar con la lectura.

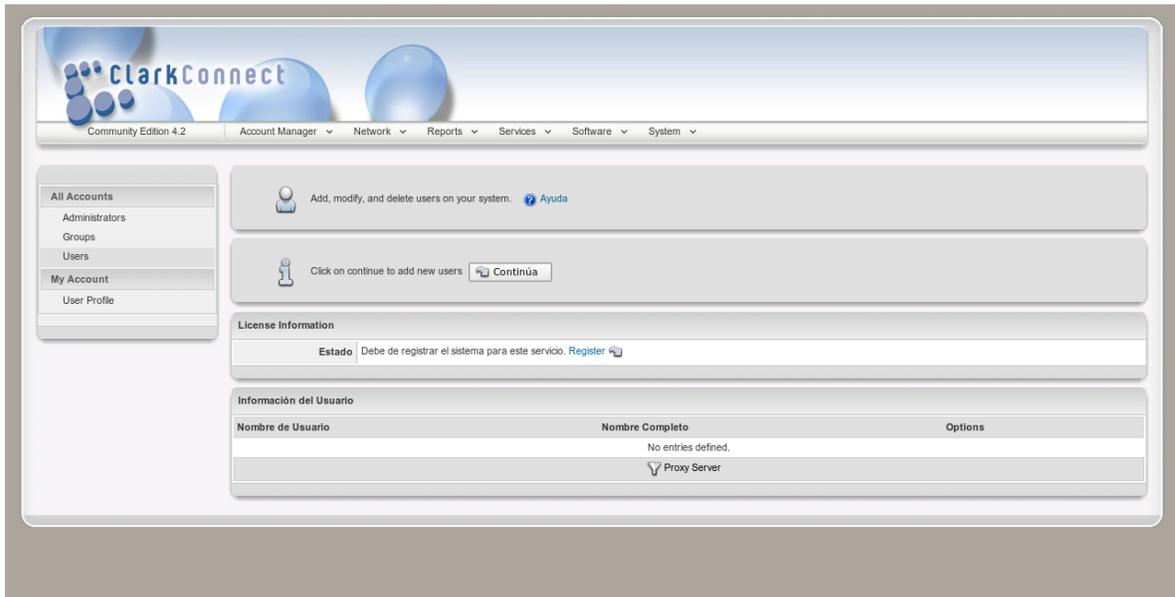
### **5.3.7 USER ACCOUNT MANAGER (ADMINISTRADOR DE CUENTAS DE USUARIO)**

La sección *Account Manger* del *Webconfig* nos permite agregar, borrar y administrar las cuentas de usuarios en el servidor, además de agrupar estas cuentas, nos permite darle permisos especiales de administración a usuarios específicos, facilitando así el manejo del *Firewall*.

#### **5.3.7.1 USUARIOS**

Desde esta interfaz podemos crear, modificar y borrar las cuentas de usuario presentes en el servidor; la cuenta de *root* es la única que no aparece en esta sección por obvias razones.

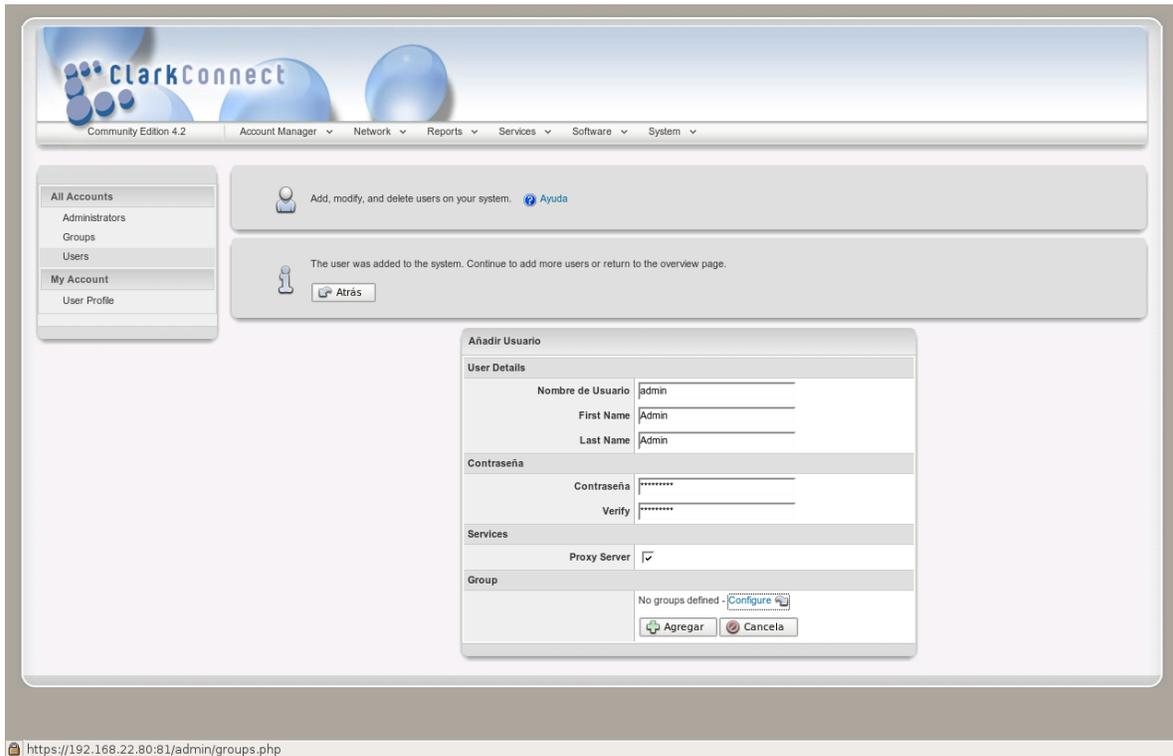
[Imagen acc1]



Adicionalmente esta sección nos muestra el estado del licenciamiento del *ClarkConnect*. Al ser una versión gratuita solo se pueden crear 10 cuentas de usuario que pueden usar correo electrónico en el servidor, las cuentas adicionales para este fin tienen que ser compradas a [pointclark.net](http://pointclark.net) a 20 USD cada una; el resto de cuentas que no usen correo no tienen restricciones.

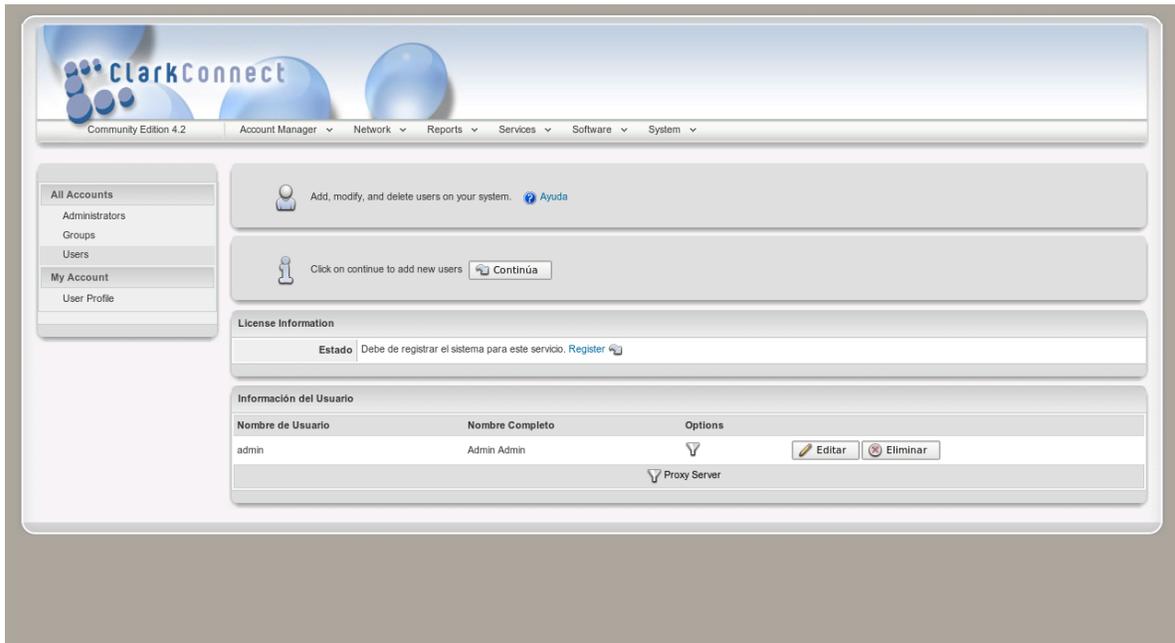
## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen acc2]



Para crear una nueva cuenta se presiona en el botón *Continue* el cual nos lleva a una nueva ventana donde especificamos los datos del nuevo usuario como: nombre de usuario, nombre real, apellido y contraseña, además de esto se puede especificar por cada usuario que tipos de servicios puede usar (*Proxy*, *Servidor de Correo*, *FTP*, etcétera) y a que grupo o grupos pertenece; finalizado esto se hace clic en *Add* para crear la nueva cuenta o *Cancel* para no hacerlo.

[Imagen acc3]



Una vez la cuenta esta creada vemos que la ventana borra el contenido que introdujimos anteriormente y nos permite crear una nueva cuenta o regresar a la sección principal donde en *User Information* (información de usuario) vemos tres características principales: nombre de usuario, nombre y apellidos y los servicios que puede usar; para cada cuenta existen dos botones que permiten editar o borrar la cuenta según sea el caso.

### **5.3.7.2 USER PROFILE**

En esta pequeña sección cualquier usuario puede ingresar al *Firewall*, por: `https://192.168.1.254:81` , ingresar su nombre de usuario y contraseña; al hacer esto accede a esta sección que le da la posibilidad de cambiar la contraseña actual por una nueva escogida por él.

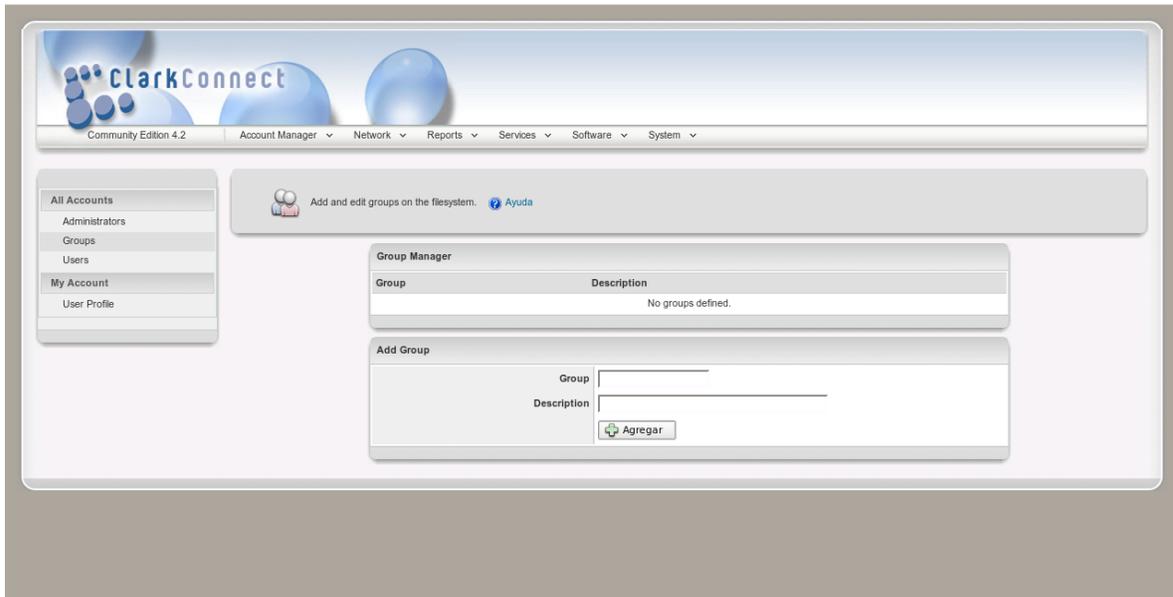
Todos los usuarios tienen acceso a esta sección del *Webconfig*, es recomendable cambiar las contraseñas de acceso por lo menos una vez al mes.

### **5.3.7.3 GRUPOS**

Como se comentó anteriormente en esta sección del *Account Manager* se pueden crear, borrar y administrar los grupos creados para mejorar el manejo de una gran cantidad de usuarios.

Al ingresar a la página se aprecia el *Group Manger*, esta sección los grupos que existen, además de una descripción y las acciones que se pueden realizar.

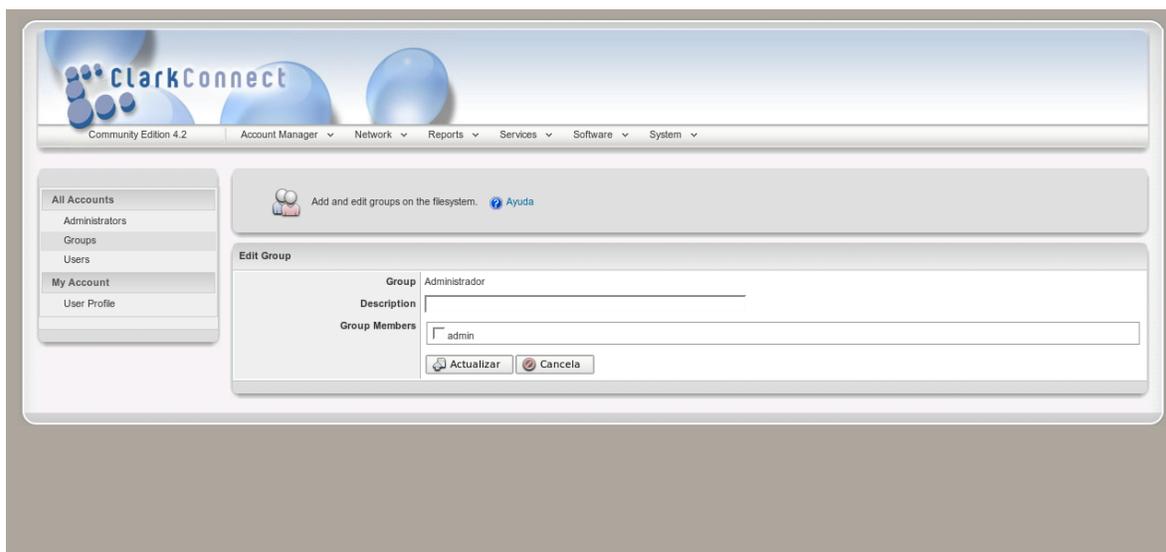
[Imagen acc4]



Para crear un grupo se escribe el nombre de este en la sección inferior junto con una descripción para facilitar la administración, al presionar Add nos lleva a una nueva ventana donde podemos seleccionar, por medio de *checkboxes*, los usuarios que van a pertenecer al grupo recién creado. (*GNU/Linux* permite asociar un usuario a múltiples grupos de trabajo, para así garantizar un correcto manejo de los permisos de seguridad). Al presionar `update` volvemos a la página principal de *Group* donde ahora aparece el nuevo grupo.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen acc5]

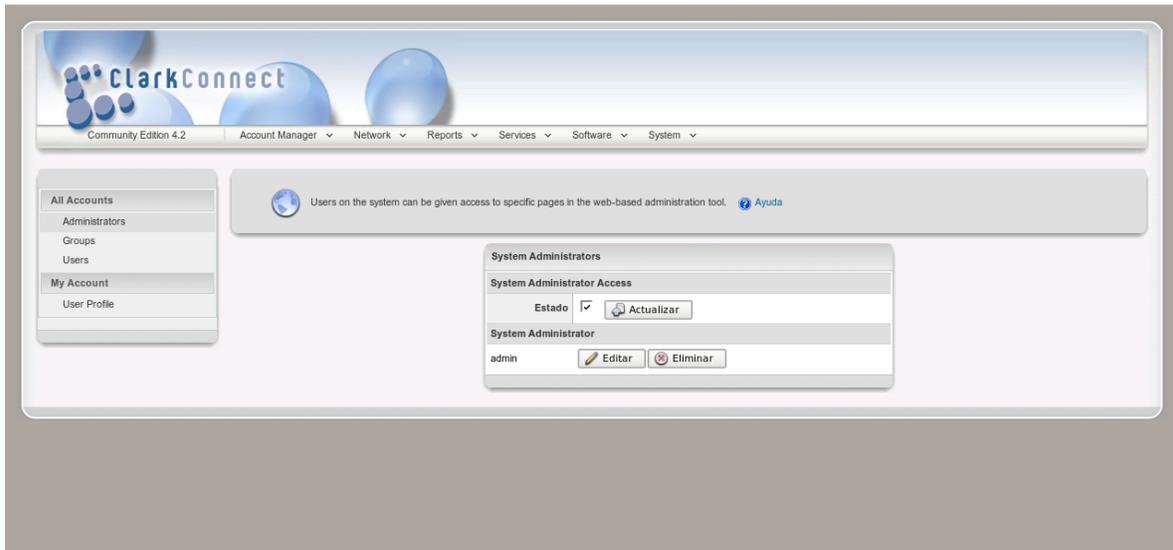


Para añadir nuevos usuarios a un grupo existente revisar nuevamente el apartado anterior, 5.3.7.1.

#### 5.3.7.4 ADMINISTRADOR

Esta sección del *Account Manager* permite añadir, eliminar y gestionar los administradores del sistema. Esto puede ser útil si se desea que otros usuarios tengas ciertos derechos para manejar el *Webconfig*, ver reportes del sistema y solucionar problemas sin estar siempre consultando con el administrador de la red.

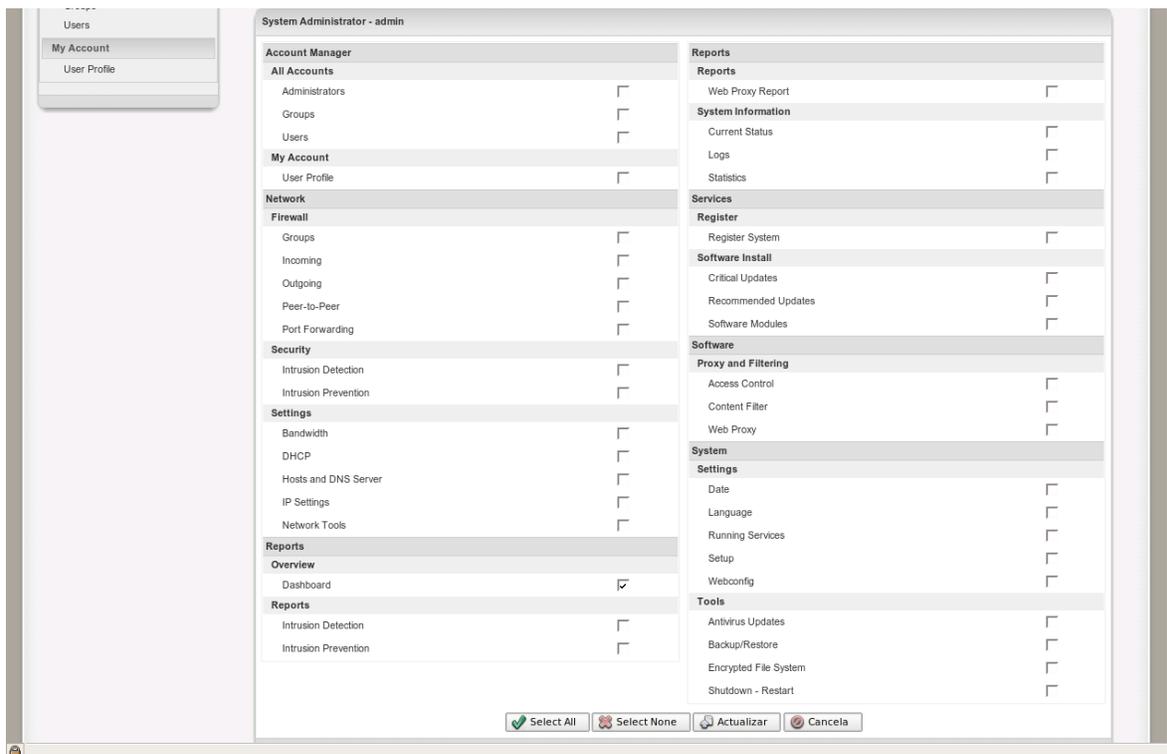
[Imagen acc6]



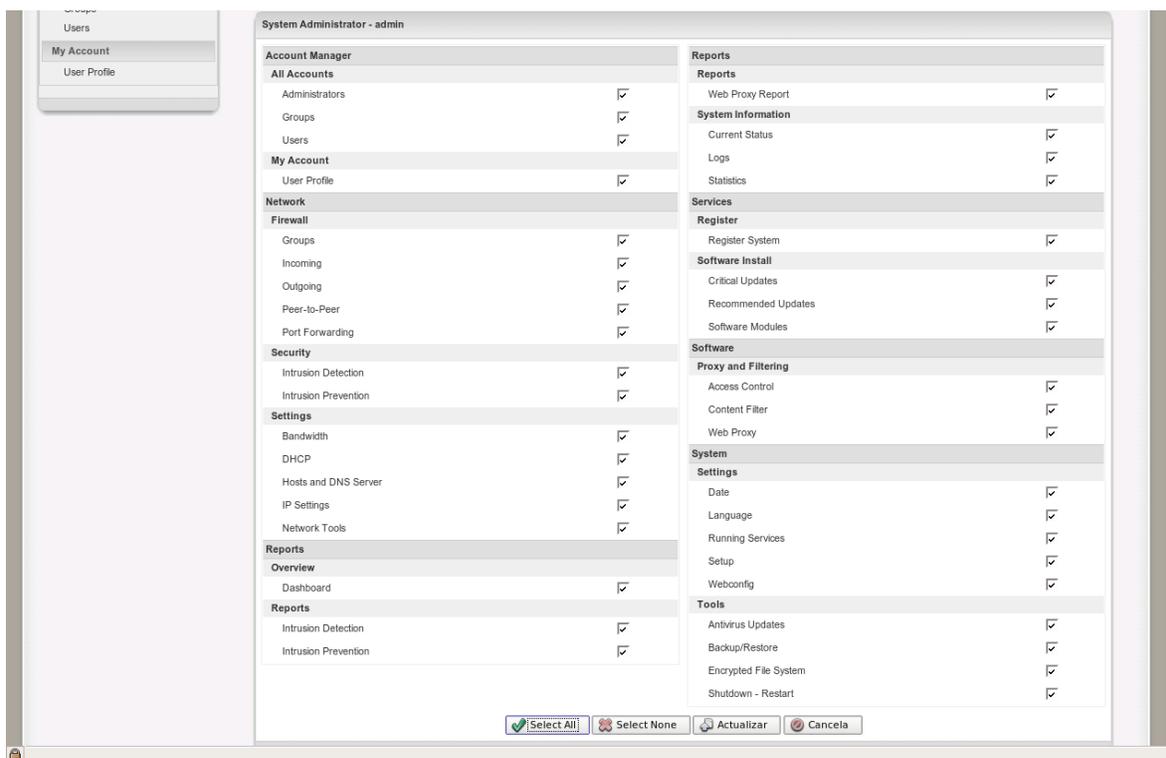
Para añadir un usuario a la lista de los administradores del sistema se selecciona el usuario de la lista desplegable y se presiona Add. Esto nos lleva a una página donde podemos seleccionar a que páginas, servicios u opciones específicos tiene el nuevo administrador. Por ejemplo: puede ser útil darle permisos para revisar algunos reportes y gestionar las cuentas de usuario, además de permitirle modificar el *Proxy* y/o filtro de contenido. Al terminar de seleccionar las páginas permitidas se presiona Update para aceptar los cambios realizados o Cancel para terminar sin realizar ningún cambio en las opciones.

# Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen acc7]



[Imagen acc8]



Terminados todos los cambios el usuario podrá inmediatamente hacer uso de sus nuevos permisos como (pseudo-)administrador del sistema.

### **5.3.8 CONTENT FILTER (FILTRADO DE CONTENIDO)**

Hemos llegado a la segunda parte clave de este trabajo escrito, el filtro de contenido que bloqueará páginas Web inapropiadas para los usuarios, además, puede ser útil para ser usado para bloquear páginas de *Webmail* como lo son `hotmail.com` o `gmail.com`, las cuales pueden interferir con las actividades normales que se realizan en una institución educativa.

Pero esto no es solo su función, el *Dansguardian* (el nombre del *software*) ayuda a mejorar la seguridad de la red impidiendo que cierto tipo de contenido peligroso ingrese a la red local.

En conclusión este filtro garantiza que la institución pueda realizar su función principal que es educar, y garantizando un contenido apropiado tanto para alumnos con empleados y profesores se generará un excelente ambiente de estudio y de trabajo.

El filtro de contenido usa una variedad de métodos que garantizan que se desempeñe de la mejor manera posible. Algunos usuarios podrán incluso encontrar formas de saltarlo, para evitar ello lo configuramos de una forma razonable y “segura”.

A continuación se describe cómo y con que métodos se filtra el contenido:

## 1. Extensión/*MIME*:

**Banned File Extensions;** esta herramienta es útil limitando las extensiones de archivo seleccionadas, garantizando así pocas probabilidades que usuarios ejecuten código peligroso arbitrariamente en máquinas de la red local. Para prohibir una extensión se seleccionan con el *checkbox* y se presiona a continuación *Update*; si la extensión buscada no aparece en la lista se puede añadir fácilmente a través del campo de texto (*Custom File Extension*).

**Banned MIME<sup>49</sup> Types;** de forma similar trabaja esta herramienta impidiendo que el contenido seleccionado no pueda ser visualizado, ya que a veces este puede ser usado para explotar vulnerabilidades del *software* en los navegadores o bien en el SO.

## 2. Site List:

**Banned Site List;** también llamada lista negra, se agregan las páginas Web, dominios o direcciones de *IP* por las cuales no se puede navegar.

**Exception Site List;** lista blanca, estos son los sitios por los cuales se esta permitido navegar a pesar de su contenido.

**Grey Site List;** lista gris, aquí se listan las páginas por las cuales se puede navegar pero no se puede descargar o subir contenido. (Ejemplo: se puede ingresar a *youtube.com* y navegar por sus páginas, pero no se podrán visualizar los videos de la página).

---

49 (*Multipurpose Internet Mail Extensions*), Extensiones de Correo de Internet.

- 3. *Phrase Lists***; aquí se especifica que tipo de contenido se desea bloquear. Como mínimo se recomienda usar el bloqueo de *Proxys*, para que los usuarios no puedan saltarse el *Dansguardian*.
  
- 4. *Blacklist***; las casillas permiten seleccionar que tipo de contenido se desea bloquear, el filtro entonces buscará que páginas Web entran dentro de las categorías seleccionadas y las bloquea.
  
- 5. *Banned User/Exempt IP List***; esta herramienta se puede usar tanto para bloquear como para permitir que las direcciones de *IP* especificadas naveguen en Internet; adicionalmente se pueden organizar las direcciones en grupos para facilitar así el manejo.

# [Imagen soft1]

The screenshot displays a web content filter configuration interface. At the top, a status bar indicates: "The web content filters web traffic on the Local Area Network. The filter engine uses a variety of methods including phrase matching, URL filtering and black/white lists." Below this, the interface is divided into two main sections: "Banned File Extensions" and "Banned MIME Types".

**Banned File Extensions:** This section contains a grid of file extensions, each with a checkbox. The extensions listed are: .ade, .adp, .asf, .asx, .avi, .bas, .bat, .bin, .bz2, .cab, .cdr, .chm, .cmd, .com, .cpl, .crt, .cue, .dll, .dmg, .doc, .exe, .gz, .hlp, .hqx, .hta, .inf, .ini, .ins, .iso, .isp, .js, .jse, .lnk, .mda, .mdb, .mde, .mdt, .mdw, .mdz, .mp3, .mpeg, .mpg, .msc, .msi, .msp, .mat, .ogg, .ops, .otf, .pcd, .pif, .prf, .rar, .reg, .scf, .scr, .sct, .sea, .sh, .shb, .shs, .sit, .smi, .sys, .tar, .tgz, .url, .vb, .vbe, .vbs, .vxd, .wmf, .wsc, .wsf, .wsh, .xls, .zip.

**Banned MIME Types:** This section contains a grid of MIME types, each with a checkbox. The MIME types listed are: application/compress, application/gzip, application/java-vm, application/x-compress, application/x-gzip, application/zip, audio/mpeg, audio/x-mpeg, audio/x-pn-realaudio, audio/x-wav, video/acorn-replay, video/mpeg, video/mxvideo, video/quicktime, video/x-mpeg2.

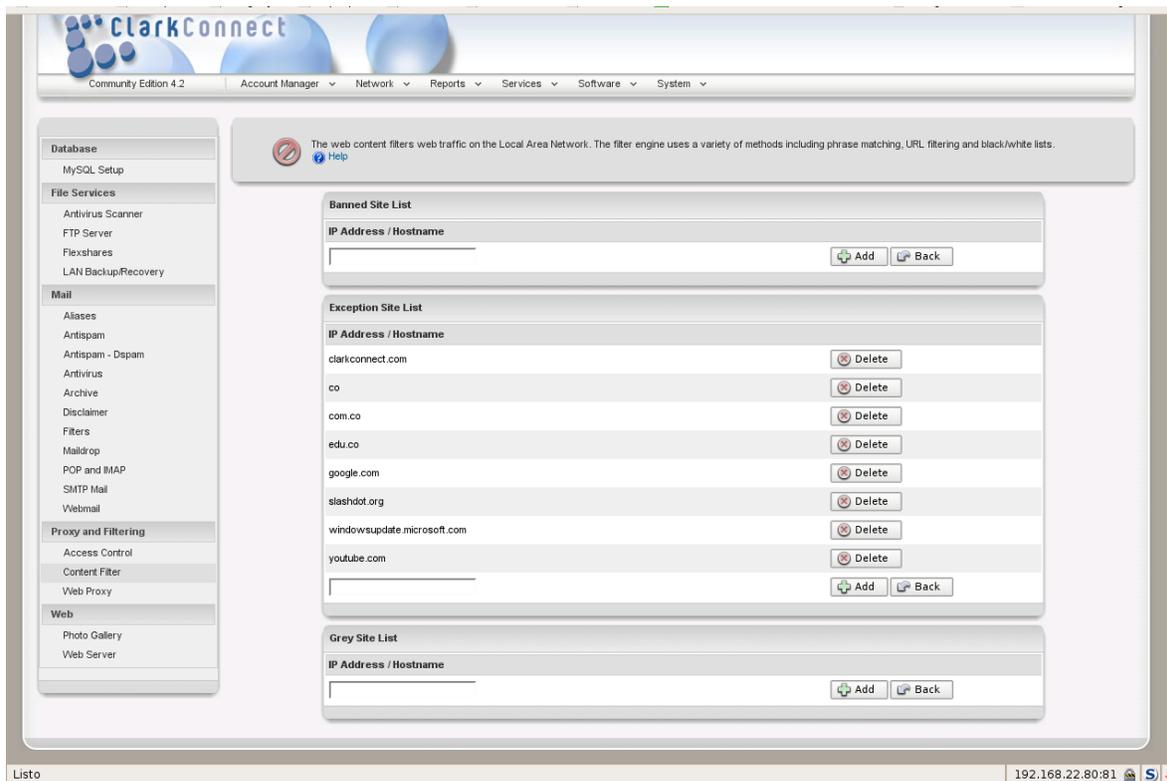
Both sections include control buttons: "Select All", "Select None", "Update", and "Back". Below these buttons is a text input field for "Custom File Extension:" and "Custom MIME Type:" with an "Add" button.

The interface also features a left-hand navigation menu with categories: Database (MySQL Setup), File Services (Antivirus Scanner, FTP Server, Flexshares, LAN Backup/Recovery), Mail (Aliases, Antispam, Antispam - Dspam, Antivirus, Archive, Disclaimer, Filters, Maildrop, POP and IMAP, SMTP Mail, Webmail), Proxy and Filtering (Access Control, Content Filter, Web Proxy), and Web (Photo Gallery, Web Server).

The bottom status bar shows the text "Listo" on the left and "192.168.22.80:81" on the right, along with system icons.

# Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen soft2]



# [Imagen soft3]

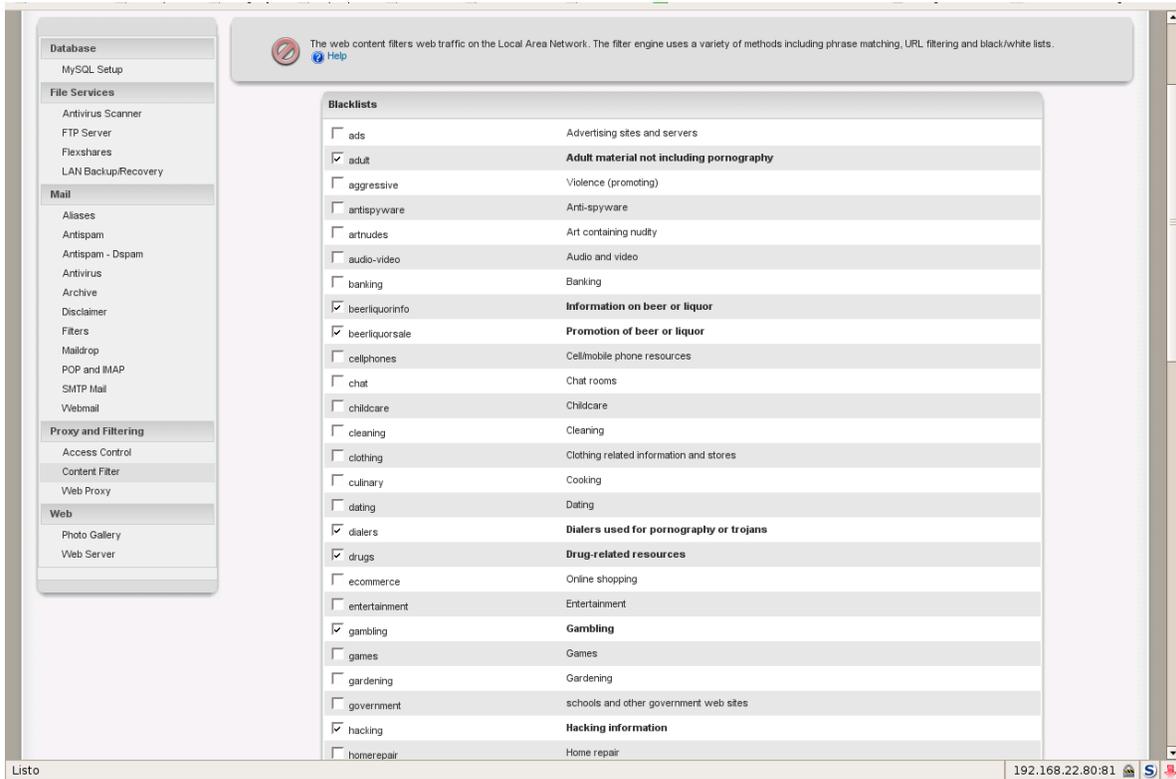
The content filter system uses phrase lists to calculate a score for every web page. You can fine tune your content filter scoring by specifying which phrase lists to use.

Phrase Lists	
<input checked="" type="checkbox"/> badwords	<b>Swear words</b>
<input type="checkbox"/> chat	Online chat
<input type="checkbox"/> drugadvocacy	Drug advocacy
<input type="checkbox"/> forums	Forums
<input type="checkbox"/> gambling	Gambling
<input type="checkbox"/> games	Games
<input checked="" type="checkbox"/> goodphrases	<b>Acceptable phrases</b>
<input type="checkbox"/> gore	Gore
<input type="checkbox"/> illegaldrugs	Illegal drugs
<input type="checkbox"/> intolerance	Intolerance
<input type="checkbox"/> legaldrugs	Legal drugs
<input checked="" type="checkbox"/> malware	<b>Viruses and malware</b>
<input type="checkbox"/> news	News
<input type="checkbox"/> nudism	Nudism
<input type="checkbox"/> peer2peer	Peer-to-peer
<input type="checkbox"/> personals	Personals
<input checked="" type="checkbox"/> pornography	<b>Pornography</b>
<input checked="" type="checkbox"/> proxies	<b>Proxy servers</b>
<input checked="" type="checkbox"/> selflabeling	<b>Self Rated Sites</b>
<input type="checkbox"/> sport	Sports
<input type="checkbox"/> violence	Violence
<input checked="" type="checkbox"/> warezhacking	<b>Illegal software and hacking</b>
<input type="checkbox"/> weapons	Weapons
<input type="checkbox"/> webmail	Webmail

Listo 192.168.22.80:81

# Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen soft4]



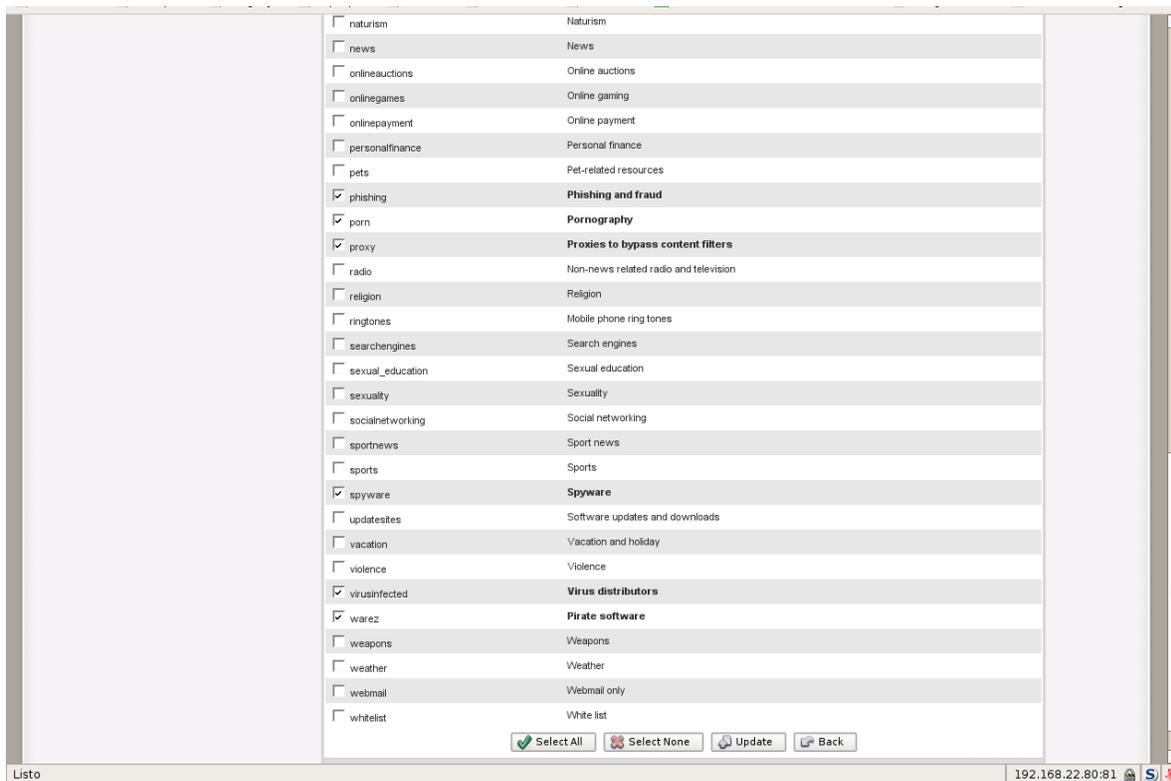
# [Imagen soft5]

<input type="checkbox"/>	instantmessaging	Instant messaging
<input type="checkbox"/>	jewelry	Jewelry information and online stores
<input type="checkbox"/>	jobsearch	Job search
<input type="checkbox"/>	kidstimestwasting	Time wasters for kids
<input type="checkbox"/>	mail	Webmail and e-mail
<input type="checkbox"/>	medical	Medical
<input type="checkbox"/>	mobile-phone	Mobile phone
<input type="checkbox"/>	naturism	Naturism
<input type="checkbox"/>	news	News
<input type="checkbox"/>	onlineauctions	Online auctions
<input type="checkbox"/>	onlinegames	Online gaming
<input type="checkbox"/>	onlinepayment	Online payment
<input type="checkbox"/>	personalfinance	Personal finance
<input type="checkbox"/>	pets	Pet-related resources
<input checked="" type="checkbox"/>	phishing	<b>Phishing and fraud</b>
<input checked="" type="checkbox"/>	porn	<b>Pornography</b>
<input checked="" type="checkbox"/>	proxy	<b>Proxies to bypass content filters</b>
<input type="checkbox"/>	radio	Non-news related radio and television
<input type="checkbox"/>	religion	Religion
<input type="checkbox"/>	ringtones	Mobile phone ring tones
<input type="checkbox"/>	searchengines	Search engines
<input type="checkbox"/>	sexual_education	Sexual education
<input type="checkbox"/>	sexuality	Sexuality
<input type="checkbox"/>	socialnetworking	Social networking
<input type="checkbox"/>	sportnews	Sport news
<input type="checkbox"/>	sports	Sports
<input checked="" type="checkbox"/>	spyware	<b>Spyware</b>
<input type="checkbox"/>	updatesites	Software updates and downloads
<input type="checkbox"/>	vacation	Vacation and holiday
<input type="checkbox"/>	violence	Violence

Listo 192.168.22.80:81

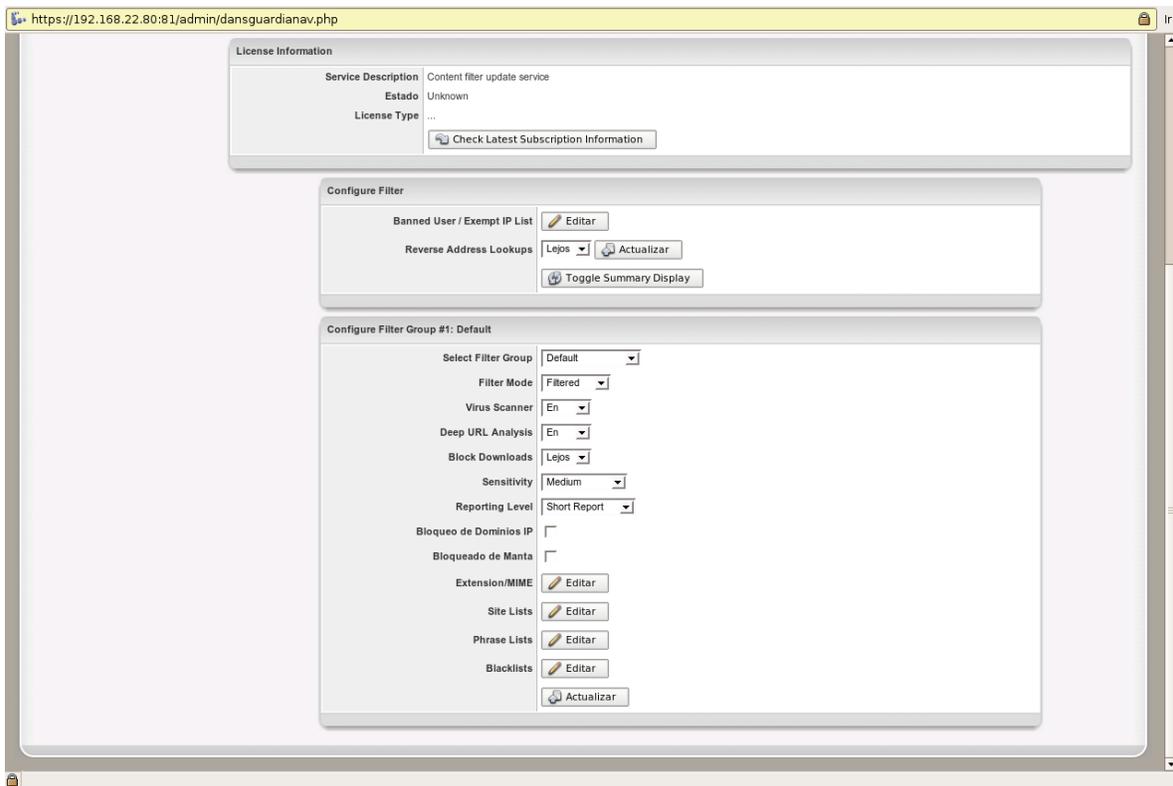
# Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen soft6]



## 5.3.8.1 CONFIGURACIÓN DEL CONTROL DE CONTENIDO

[Imagen soft7]



Para mejorar el control del contenido se pueden crear grupos de usuarios, con lo cual se puede personalizar el filtro. Para crear un grupo se selecciona del menú desplegable `Select Filter Group` la opción `Add Filter Group`. Esto nos lleva a una página donde escribimos el nombre del nuevo grupo, posteriormente volvemos a la sección anterior

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

pero ahora se puede configurar por separado un grupo específico de usuarios. Crear un grupo para filtrar no es obligatorio ni necesario, es únicamente una utilidad de la cual se puede sacar provecho, si no queremos crear un grupo específico de usuarios el grupo `Default` será el predeterminado para aplicar las reglas de filtrado.

`Filter Mode` nos permite escoger que acción deseamos realizar cuando el tráfico pasa por el *Proxy*: Prohibirlo (*Banned*), filtrarlo (*Filtered*) y no filtrarlo (*Unfiltered*). Escogemos filtrarlo y pasamos al siguiente menú *Virus Scanner*, esta opción solo funcionará si se tiene instalado el módulo de antivirus.

La función del `Deep URL Analysis` consume mucha memoria *RAM*, en máquinas con pocos recursos se recomienda desactivar esta función y en su reemplazo mejorar y extender las entradas de la lista negra.

La opción para bloquear las descargas (`Block Downloads`) que pasan por filtro puede ser útil, pero es muy restrictiva, se recomienda usar la opción del *Web Proxy* para esa función, apartado 5.3.3.

Para configurar la sensibilidad con que el filtro de contenido funcionará se selecciona una de las seis opciones. De esta sensibilidad dependerá cuantas páginas y que tipo de contenido será bloqueado. Se recomienda inicialmente `Medium` para así ajustar las preferencias a las necesidades propias.

El nivel de reporte (`Reporting Level`) indica que tipo de aviso se le

mostrará al usuario cuando una página que desea acceder sea bloqueada. *Short Report* es suficiente para mostrarle al usuario que pretende visitar contenido indebido; existe la opción de crear una plantilla de una página para mostrar un mensaje personalizado (*Custom Report*), pero ese tema no será tratado en este trabajo.

Una forma común de saltarse los filtros de contenido es reemplazando el dominio del sitio Web por su dirección de *IP*; al activar *Block IP Domains* todas las peticiones realizadas a la dirección de *IP* serán bloqueadas, a menos que se especifique lo contrario en la lista blanca (*Exception List*).

*Blanket Block* es la opción más restrictiva de todas, si se activa, se bloquearán todas las páginas Web que se intenten visitar a excepción de las especificadas en la lista blanca; puede ser útil en lugares públicos como bibliotecas.

Es normal ver algunos sitios Web rotos, desordenados o que no se pueden ver parcialmente, esto se debe a que el filtro de contenido puede bloquear secciones de las páginas Web si considera que su contenido es indebido o peligroso.

Configurar el *Dansguardian* puede demorar varios días o semanas, se puede seleccionar una configuración inicial, pero es posible que haya que acomodarla mejor a las necesidades de la institución y a los problemas que hayan tenido los usuarios. Esta es una herramienta que

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar es necesario actualizar constantemente.

### **5.3.9 REPORTE**

La sección *Reports* del *Webconfig* nos brindará información actualizada y en tiempo del del estado del sistema, sus configuraciones y servicios adicionales.

Es recomendable visitar constantemente esta sección, para revisar, comparar datos y encontrar posibles problemas con el sistema. De hecho cada vez que iniciamos sesión como *root* en el *Webconfig* nos lleva al *Dashboard*, el cual funciona como un tablero donde se muestra información actual y relevante del sistema.

### 5.3.9.1 DASHBOARD (TABLERO)

El Dashboard nos permite echarle al sistema un vistazo rápido de su estado actual, como lo es, la dirección de IP pública y privada, la configuración del idioma, el número de usuarios registrados en el sistema, y si se tiene instalado el módulo de de prevención de intrusos se mostrarán los últimos eventos ocurridos.

[Imagen rep1]

The screenshot shows the ClarkConnect dashboard interface. At the top, there is a navigation menu with options: Account Manager, Network, Reports, Services, Software, and System. The main content area is divided into several sections:

- Overview:** A summary section with a globe icon and the text "The following is an overview of current settings and data." with a link to "Ayuda".
- System Overview:** A table showing system settings:

Sistema Tiempo	Apr 11 2008 14:34:31 COT (America/Bogota)	<a href="#">Editar</a>
Language	Spanish - es_ES	<a href="#">Editar</a>
Number of Users	1	<a href="#">Editar</a>
- Interface:** A table showing network interface details:

Role	Tipo	Protocolo de Inicio	Dirección IP	Link	Speed	
eth0	External	Ethernet	DHCP	IP PÚBLICA	SI	100 Mb
eth1	LAN	Ethernet	Estático	192.168.22.80	SI	100 Mb

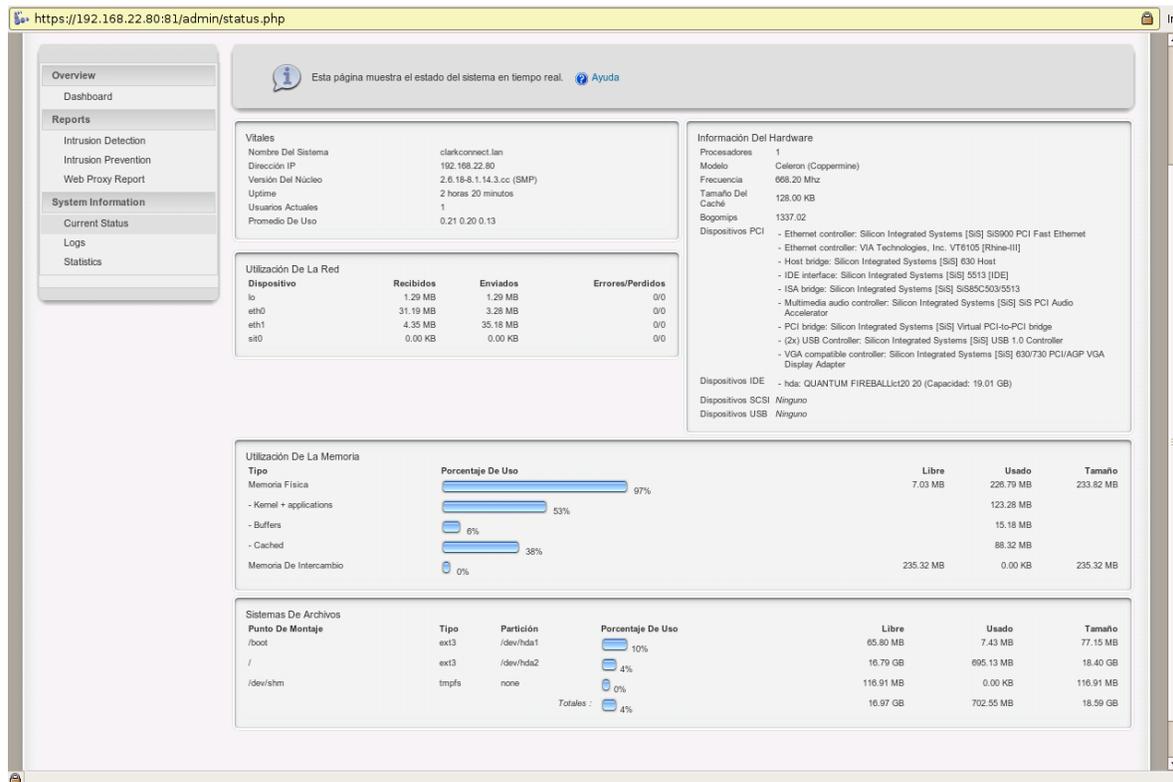
A sidebar on the left contains a menu with categories: Overview, Reports, and System Information, each with sub-items.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

### 5.3.9.2 CURRENT STATUS (ESTADO ACTUAL DEL SISTEMA)

Como su nombre lo dice, por medio de pequeños pero intuitivos y sencillos reportes, nos muestra el estado actual del sistema.

[Imagen rep2]

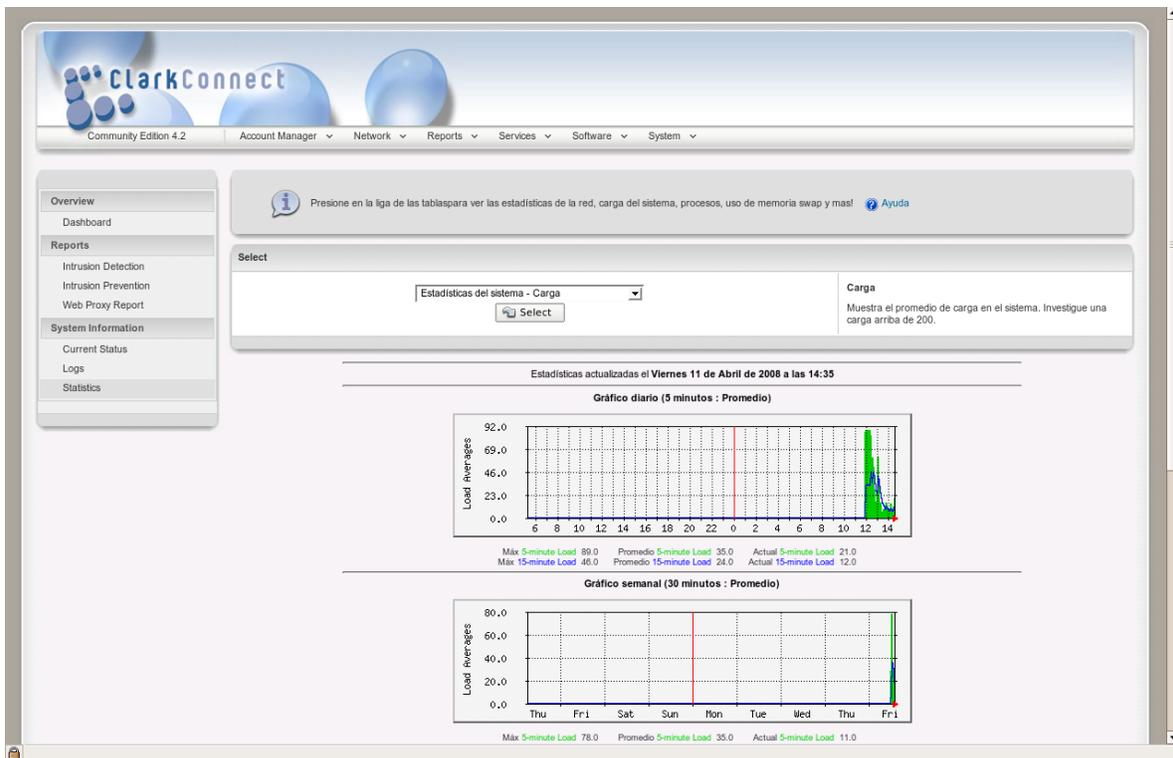


La página es dividida en secciones cada una con información diferente:

1. *System Vital*, información vital del sistema.
2. *Network Usage*, uso de las interfaces de red.
3. *Hardware Information*, muestra los dispositivos de *hardware* que existen en el sistema
4. *Memory Usage*, muestra el consumo de memoria dividido en secciones. Es conveniente revisar esta sección constantemente.
5. *Mounted Filesystems*, información sobre los sistemas de archivos montados en el servidor.

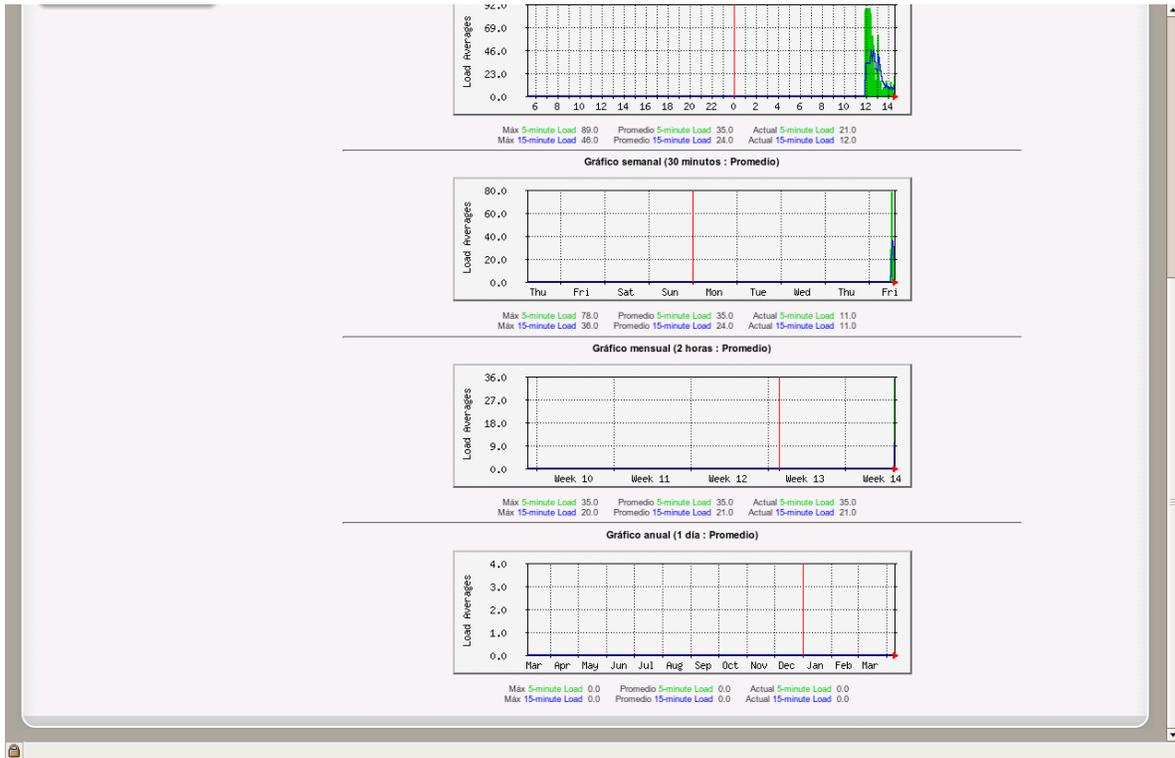
### 5.3.9.3 STATISTICS (ESTADÍSTICAS)

[Imagen rep3]



Información histórica del rendimiento del sistema por medio de gráficas, las cuales muestran a su vez la información: Máxima, Promedio y Actual (*Maximum, Average, Current*).

[Imagen rep4]



Se usan datos de diferentes periodos para generar las gráficas, para así estudiar de una forma sencilla y comprensible el estado y el comportamiento del sistema en los periodos:

### 5.3.9.3.1 TIPOS DE ESTADÍSTICAS

1. **Load**, la carga del sistema es una medida promedio de cómo funciona el conjunto del todo que conforma al sistema en un periodo de tiempo; se da por entendido que la carga del sistema es el uso que se le da al procesador (*CPU*), pero este es solo uno de los factores, el exceso de escritura en el disco duro, muchos procesos cargados en memoria, todo esto y más en conjunto es la carga del sistema. Esto nos sirve para conocer en que tiempos del día, por ejemplo, el servidor tiene una carga fuerte o si él trabaja en exceso y se necesita buscar una solución para evitar el desgaste prematuro del *hardware*.

En las gráficas se muestran dos líneas, la verde se usa para indicar el promedio en un periodo de cinco minutos; la línea azul muestra el promedio en un periodo de quince minutos.

Daily Graph (*5 Minute Average*); (Diario, promedio cinco minutos).

Weekly Graph (*30 Minute Average*); (Semanal, promedio de treinta minutos).

Monthly Graph (*2 Hour Average*); (Mensual, promedio de dos horas).

Yearly Graph (1 Day Average); (Anual, promedio de un día).

“Una carga sostenida por encima de 200 en la tabla indica una sobrecarga del sistema (picos ocasionales por encima de este número son normales)<sup>50</sup>”.

2. *Open Connections*, se muestran gráficamente las conexiones abiertas existentes o las que ya se cerraron. Estas gráficas pueden ser de utilidad para conocer si se ha sufrido de un *DoS*<sup>51</sup> o se tiene un servicio o un programa que abre constantemente muchas conexiones al Internet.

Se muestran cuatro gráficas cada una para cuatro periodos de tiempo diferentes, diario, semanal, mensual y anual. Cada gráfica calcula un punto máximo, uno promedio y uno actual.

3. *Processes*, muestra el número de procesos corriendo en el sistema. Útil para saber a que horas del día corren mas procesos en el servidor.

Son cuatro gráficas las cuales muestran en cuatro periodos de tiempo los procesos corriendo en el servidor, la línea verde muestra el promedio total del número de procesos; la línea azul muestra el promedio actual de procesos para comparar con la línea verde y el histórico.

---

50 Cita de: [http://www.ClarkConnect.com/docs/Reports\\_-\\_Statistics](http://www.ClarkConnect.com/docs/Reports_-_Statistics)  
51 *DoS* (Ataque de denegación de Servicio, *Denial of Service*)

4. **Swap Memory**, el uso de la memoria de intercambio muestra la relación directa del uso de la memoria *RAM* en el servidor; a mayor uso y consumo de la memoria *RAM* aumenta la necesidad de usar la memoria de intercambio. Esto no es bueno, si ve un uso constante de la *swap*, y esta consume constantemente cientos de *Megabytes*, es recomendable mejorar la memoria *RAM* aumentando su capacidad y desactivar procesos y servicios innecesarios en el servidor.

La línea verde de las gráficas muestra la cantidad de memoria de intercambio disponible; la línea azul indica la cantidad de memoria de intercambio usada, a esta línea es a la que es necesario vigilar constantemente, si aumenta mas del 75% del total es necesario tomar las medidas arriba mencionadas.

Los servicios de filtrado de contenido y detección de intrusos son dos de los que mas memoria y recursos en un sistema usan.

**Nota:** “En un sistema *Linux*, la memoria *RAM* inutilizada es usada para optimizar el acceso al sistema de archivos. No debe ser sorpresa encontrar el uso de la memoria *RAM* en un 95% o superior<sup>52</sup>”.

5. **Uptime**, muestra el tiempo que lleva el servidor funcionando

---

52 Cita de: [http://www.ClarkConnect.com/docs/Reports\\_-\\_Statistics](http://www.ClarkConnect.com/docs/Reports_-_Statistics)

desde que fue reiniciado o apagado la última vez. Con estas gráficas se puede estimar el tiempo que el servidor lleva en funcionamiento; cuando fue apagado, ya sea por mantenimiento, rutina o un accidente; y calcular el costo de la energía consumida por el servidor.

Las gráficas muestran dos líneas; la línea verde representa el tiempo total desde el inicio del sistema y la línea azul el tiempo que el servidor lleva desocupado.

6. **Interfaces de red (para cada una *eth0*, *eth1*)**, muestra las estadísticas de cada interfaz de red existente en el servidor, muestra los datos del tráfico de red de entrada/salida (*incoming/outgoing*) en *kB/s*. Estos datos nos muestran a que horas del día se consume un mayor ancho de banda, de igual forma puede ayudar a detectar *DoS*, o descargas de contenido ilegal.

Las gráficas de los cuatro periodos muestran las estadísticas diarias, semanales, mensuales y anuales. La línea verde muestra el tráfico de red entrante y la línea azul muestra el tráfico saliente de cada interfaz.

Comparar y estudiar los datos provenientes de todas las gráficas puede ser de utilidad para conocer el estado actual y pasado del sistema y poder predecir el comportamiento del servidor en el futuro; además de

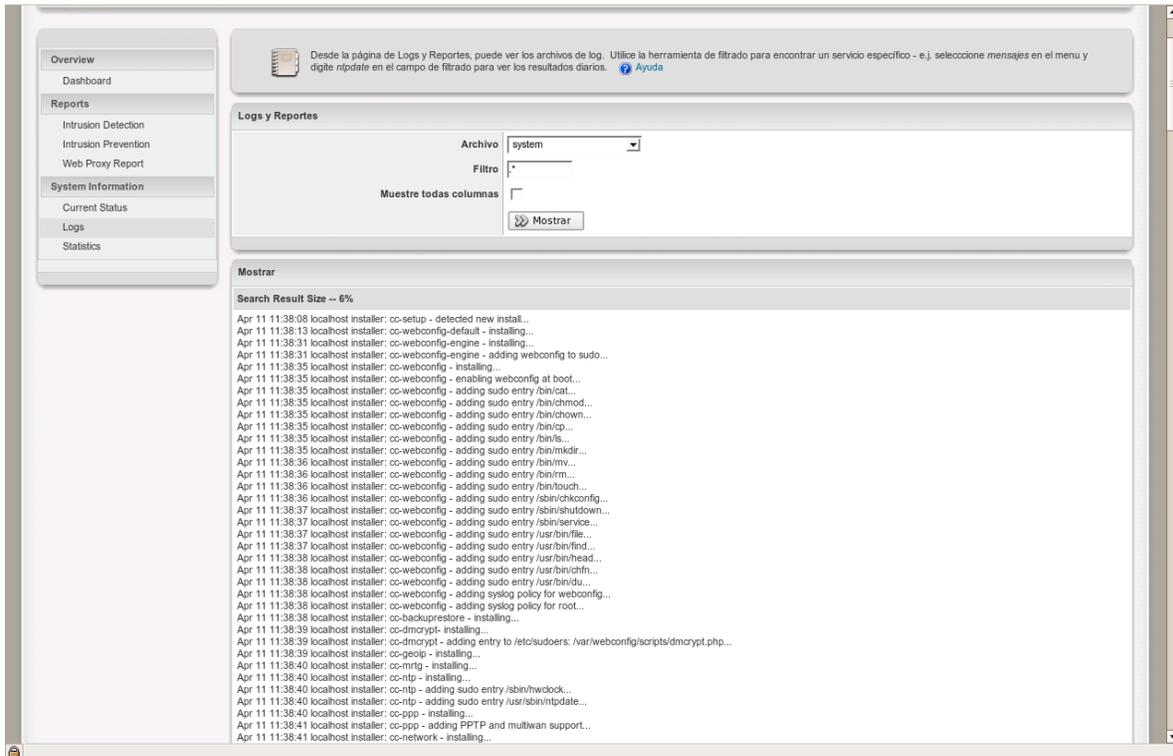
Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

la posibilidad de detectar posibles problemas antes que una falla mayor ocurra.

#### **5.3.9.4 LOGS (REGISTROS)**

En esta página se pueden ver y revisar detalladamente los registros (*logs*) del sistema; la mayoría de los servicios y algunos procesos graban en un archivo de registro (*Log file*) los sucesos ocurridos, estos pueden ser de cualquier tipo, información básica del funcionamiento, errores, conexiones nuevas, usuarios que se conectan al servidor, etcétera. Esta es una herramienta muy poderosa, pero difícil de manejar, requiere práctica y saber lo que se busca. Todo buen administrador de un sistema dedica una parte de su tiempo a revisar estos registros en busca de anomalías, errores y situaciones sospechosas, que puedan comprometer al sistema. Junto con las gráficas estos archivos maximizan la visión del estado del sistema permitiendo ver como cada componente, servicio o proceso se comporta en diferentes situaciones presentes en el día a día de un servidor.

[Imagen rep5]



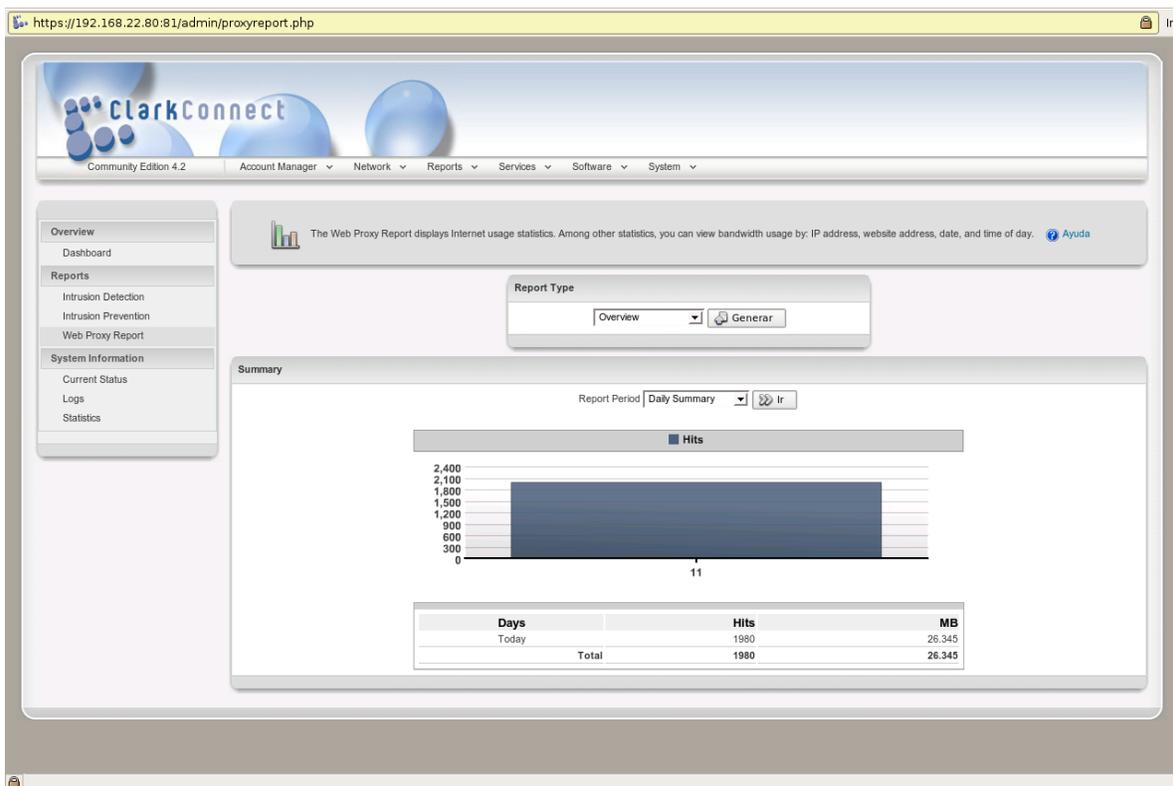
Para visualizar un registro se debe seleccionar del menú desplegable, a continuación si se desea buscar algo en especial, como por ejemplo un error, o lo concerniente al superusuario *root*, se debe de escribir en *Filter* reemplazando lo existente. Para obtener mas información se selecciona *Show Full Line* y finalmente se presiona *Display* para visualizar el archivo de registro.

Si por alguna necesidad se necesita realizar una copia (de seguridad) de estos *logs* la mayoría se encuentran en el directorio: `/var/log/` .

### 5.3.9.5 WEB PROXY REPORT

En esta página se muestran todas las conexiones, eventos y estadísticas del Proxy y el filtro de contenido, además de eso se puede visualizar el ancho de banda usado, la dirección de IP de la cual proviene la petición, los sitios web visitados y la fecha de los accesos a Internet.

[Imagen rep6]



La página de los reportes se divide en dos secciones, una para

seleccionar el reporte que se desea ver y la otra el reporte seleccionado que a su vez puede dar opciones adicionales para visualizar las estadísticas.

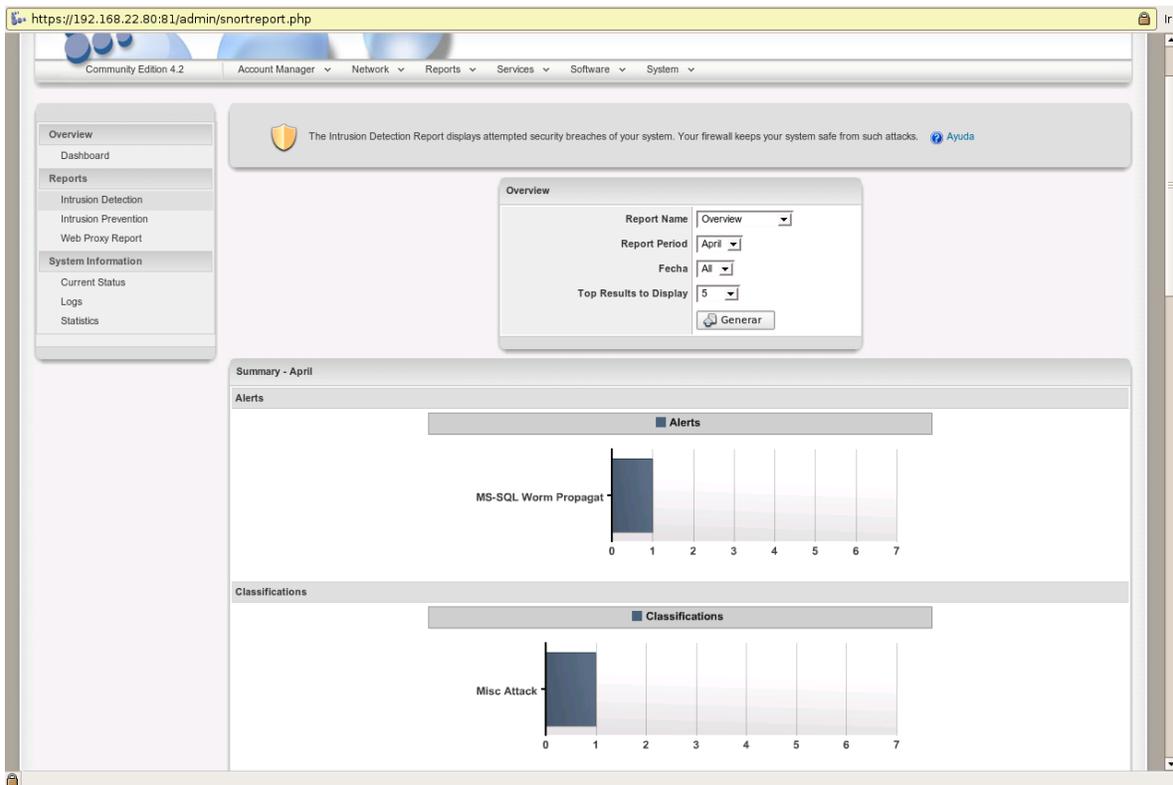
1. *Overview*, vista general de las estadísticas, para el reporte/resumen diario (*Daily Summary*) muestra una gráfica de los últimos treinta días y las peticiones (*Hits*) a páginas de Internet realizadas para cada día de este periodo, en la parte inferior se muestran los mismos datos en texto plano para una mejor comparación. Los informes mensuales, que se pueden ver seleccionando del menú desplegable la opción *Monthly Summary*, se manejan de igual forma que los anteriores.
2. *User/IP Summary*, genera un reporte mostrando que direcciones de *IP* realizaron peticiones para navegar a través del *Proxy*. Si se selecciona la opción de usuario (*Username*) se puede ver que usuarios realizaron cuantas peticiones. La opción *Hostname* permite ver el nombre de las máquinas que realizan las peticiones de páginas web. Los reportes se pueden organizar por periodos.
3. *Domain Summary*, muestra en una gráfica los dominios mas visitados según las veces que se han accedido y cuanto caché ha sido usado para realizar esta acción. Se puede escoger un periodo de tiempo y una cantidad de resultados para generar una gráfica según lo deseado.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

### 3.5.9.6 INTRUSION DETECTION (DETECCIÓN DE INTRUSOS)

Si se instaló o se desea instalar el módulo de detección e intrusión de intrusos se debe seguir con los dos capítulos siguientes, de lo contrario se recomienda saltar al apartado 3.9.10.

[Imagen net7]



En la página de los reportes del *Snort*, el programa que detecta

potenciales intrusos en la red, se puede ver la información necesaria para estudiar y analizar el tráfico potencialmente peligroso y hostil que entra a la red.

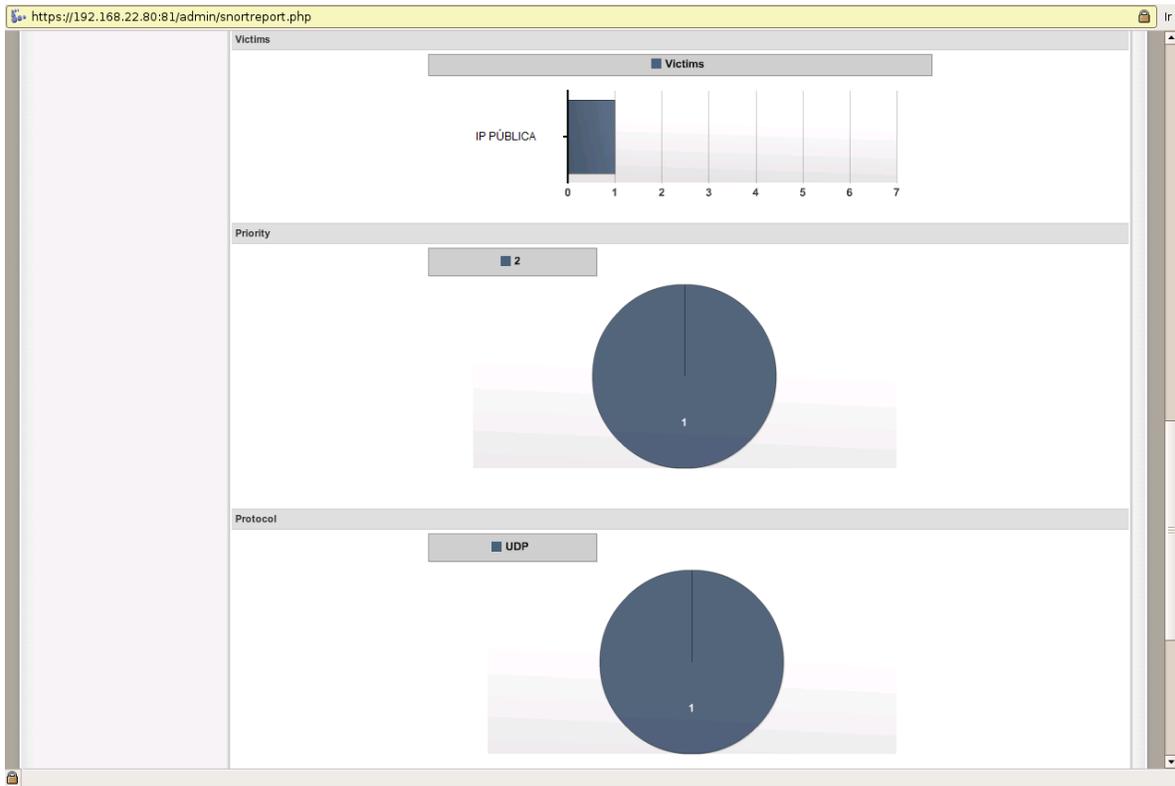
[Imagen rep8]



No es sorpresa que diariamente exista algún tipo de ataque, en realidad es inusual y raro que no suceda ninguno a lo largo del día, el tráfico hostil es pan de cada día en Internet y es una de las razones de porque los *Firewalls* son necesarios.

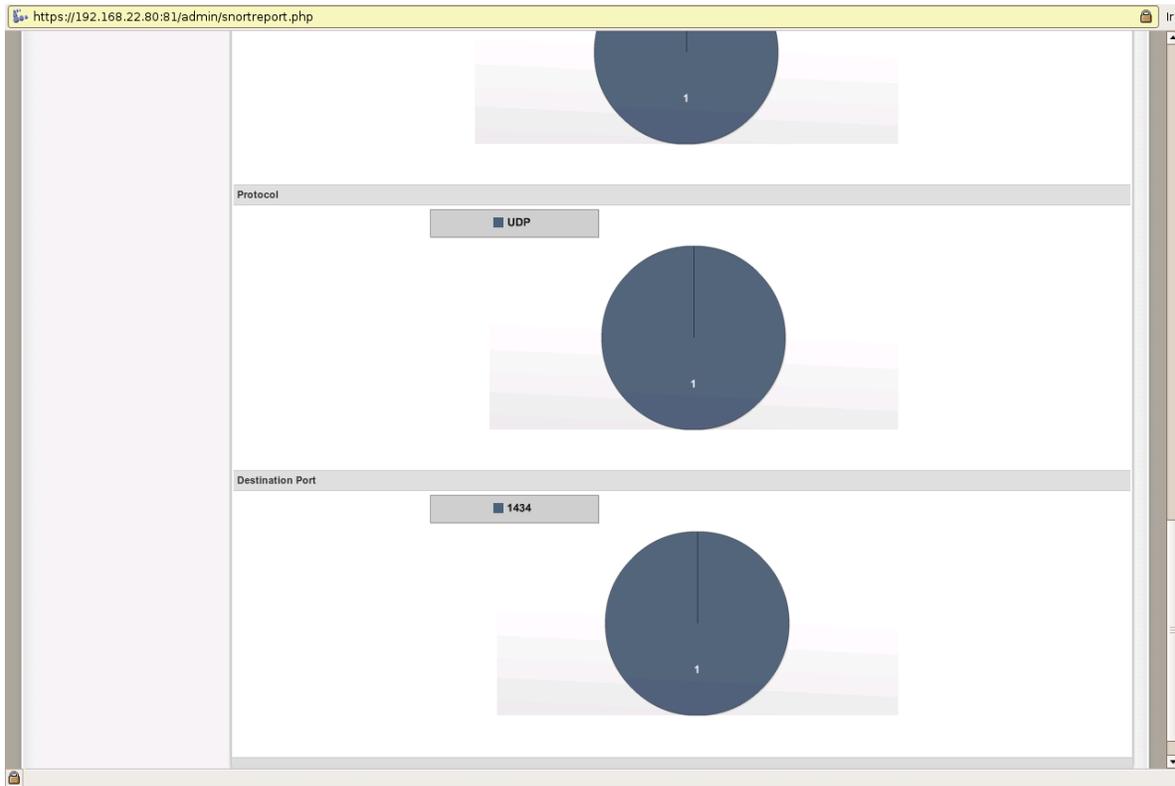
## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen rep9]



Inicialmente se muestra un reporte general de los últimos eventos en el mes actual. Para una mayor profundidad se puede aumentar el número de resultados que se mostrarán modificando el `Top Results to Display`.

[Imagen rep10]



El reporte inicial se divide en ocho secciones:

1. **Alertas (*Alerts*)**, aquí se muestran las últimas alertas generadas por el *Snort*, una gráfica muestra el nombre de la alerta que generalmente dice el tipo de evento ocurrido y el número de alertas generadas para cada evento.
2. **Clasificaciones (*Classifications*)**, agrupa los eventos en diferentes clasificaciones para así entender mejor lo sucedido.
3. **Fecha (*Date*)**, despliega en una gráfica el número eventos

ocurridos para cada día del mes actual.

4. *Atacantes (Attackers)*, muestra las direcciones de *IP* de donde provienen los últimos ataques, también muestra el número de ataques realizados por cada *IP*.
5. *Víctimas (Victims)*, una gráfica donde se exponen las direcciones de *IP* víctimas de ataques y el número de estos para cada *IP*.
6. *Prioridad (Priority)*, es el nivel por el cuál se clasifican los ataques; el nivel 1 (uno) es la prioridad mas alta, por ende un ataque mas peligroso, el nivel 3 (tres) es el de mas baja prioridad. La gráfica de torta usa estadísticas para mostrar los datos.
7. *Protocolo (Protocol)* más usado para realizar los intentos de ataque contra el servidor. Se usan estadísticas para mostrar los resultados.
8. *Puerto destino (Destination Port)* al cual llegan los ataques realizados por los atacantes, los resultados se muestran en base a estadísticas.

Para conocer más acerca de alguno de los resultados, dado que un evento es sospechoso o por otras razones, se puede seleccionar del menú desplegable *Report Name* la sección a revisar mas detalladamente, escoger un periodo para el reporte, generalmente por meses, luego una fecha si así se desea y finalmente el número de reportes a mostrar; se muestra el reporte presionando *Generate*.

“En definitiva, pese a todas las facilidades y automatizaciones y como

casi todas las herramientas de seguridad, es un apoyo que no puede sustituir la tarea del responsable de seguridad que es quien debe analizar toda la información de forma minuciosa y continuada<sup>53</sup>”.

Para configurar este módulo nos dirigimos a la pestaña `Network` y luego a `Intrusion Detection`. Desde allí podemos establecer el estado (`Running`, `Stop`) y seleccionar que políticas de detección deseamos implementar. El proceso es simple, se selecciona una regla y se presiona `Update` para hacer efectivo el cambio.

El módulo usa mucha memoria *RAM* para realizar su función, si se detecta que el sistema es lento y/o consume mucha memoria es recomendable detener este módulo.

Todos los días se crean nuevos vectores de ataque, y mantener una base de datos de estos métodos de ataque es responsabilidad del administrador de la red, en `www.snort.org` se encuentra mas información al respecto; se recomienda inscribirse en la página para descargar la lista de reglas actualizadas para mantener el servidor al día y seguro ante muchos ataques. El *ClarkConnect* brinda la posibilidad de actualizar automáticamente actualizaciones para el *Snort*, pero para ello se requiere pagar una mensualidad.

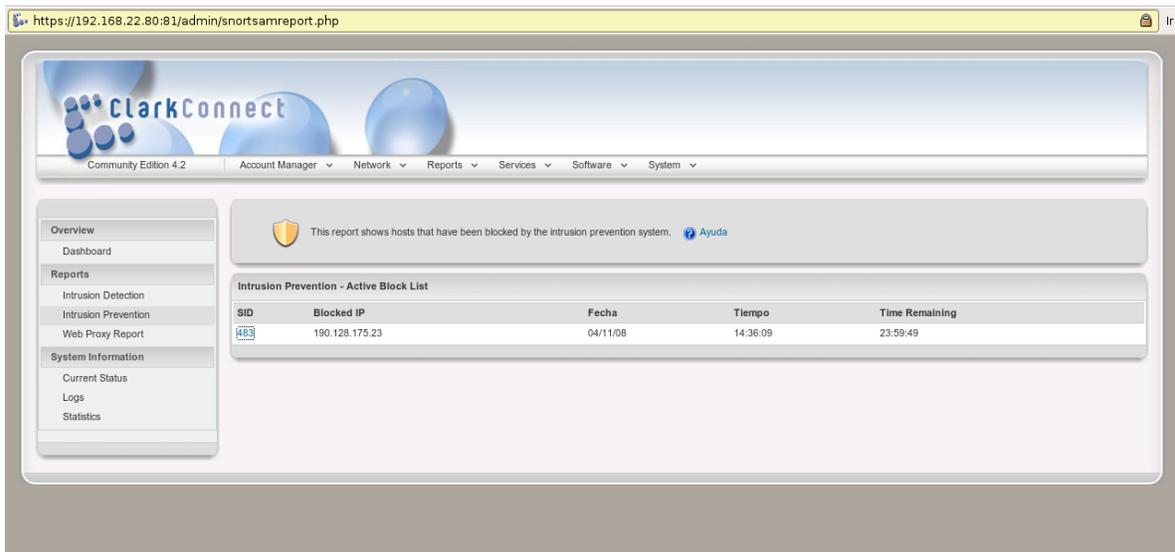
---

53 Cita de: <http://euitio178.cccu.uniovi.es/wiki/index.php/Snort>

### 3.5.9.10 INTRUSION PREVENTION (PREVENCIÓN DE INTRUSOS)

En esta página se muestran los reportes generados por el módulo para la prevención de intrusos que se encarga de bloquear atacantes y sospechosos que intentan vulnerar el sistema.

[Imagen rep11]



The screenshot shows the ClarkConnect web interface. The browser address bar displays 'https://192.168.22.80:81/admin/snortsamreport.php'. The page header includes the ClarkConnect logo and navigation menus for 'Community Edition 4.2', 'Account Manager', 'Network', 'Reports', 'Services', 'Software', and 'System'. A left sidebar contains a navigation menu with categories: 'Overview' (Dashboard), 'Reports' (Intrusion Detection, Intrusion Prevention, Web Proxy Report), and 'System Information' (Current Status, Logs, Statistics). The main content area features a shield icon and a message: 'This report shows hosts that have been blocked by the intrusion prevention system.' Below this is a table titled 'Intrusion Prevention - Active Block List' with the following data:

SID	Blocked IP	Fecha	Tiempo	Time Remaining
483	190.128.175.23	04/11/08	14:36:09	23:59:49

Se puede apreciar una lista llamada Active Block List, la cual muestra seis informaciones importantes referentes a direcciones de IP que han sido bloqueadas (debido a tráfico inapropiado o peligroso):

1. `ID`, es un identificador que se asocia al evento ocurrido, el cuál puede ser usado como hipertexto para obtener información mas detallada del suceso.
2. `Blocked IP`, esta es la dirección de *IP* bloqueada de donde se originó el ataque.
3. `Date`, la fecha del evento ocurrido.
4. `Time`, la hora.
5. `Time Remaining`, este es el tiempo restante (para llegar a 0) para que la dirección de *IP* sea desbloqueada. Normalmente el bloqueo dura veinticuatro horas.

Al ingresar a la sección de configuración de este módulo, por `Network > Intrusion Prevention`, se tiene otra breve vista de las últimas direcciones de *IP* bloqueadas, solo que desde aquí si el caso lo amerita, podemos desbloquear la dirección de *IP* presionando `Exempt List`; así la *IP* se guardará permanentemente en una lista blanca. Esto puede ser útil por ejemplo, si una dirección de *IP* necesita conectarse a nuestro servidor constantemente y para ello usa métodos que pueden resultar sospechosos. También es posible ingresar manualmente una *IP* a la lista blanca.

Si se desea borrar una dirección de *IP* de la lista sospechosa se presiona

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

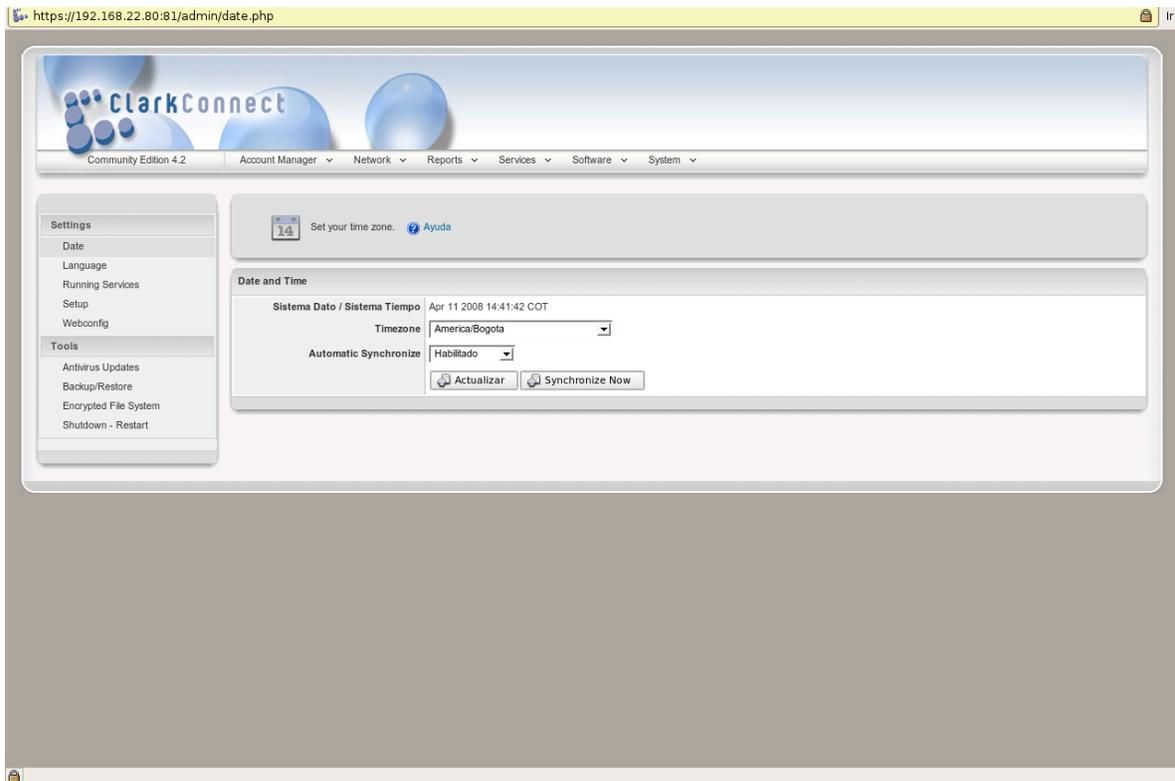
Delete y para borrar completamente esta lista se debe presionar en Reset.

## 5.3.10 SYSTEM SETTINGS (SISTEMA)

En esta sección del *Webconfig* podemos configurar y administrar de una forma sencilla el servidor.

### 5.3.10.1 FECHA

[Imagen sys1]

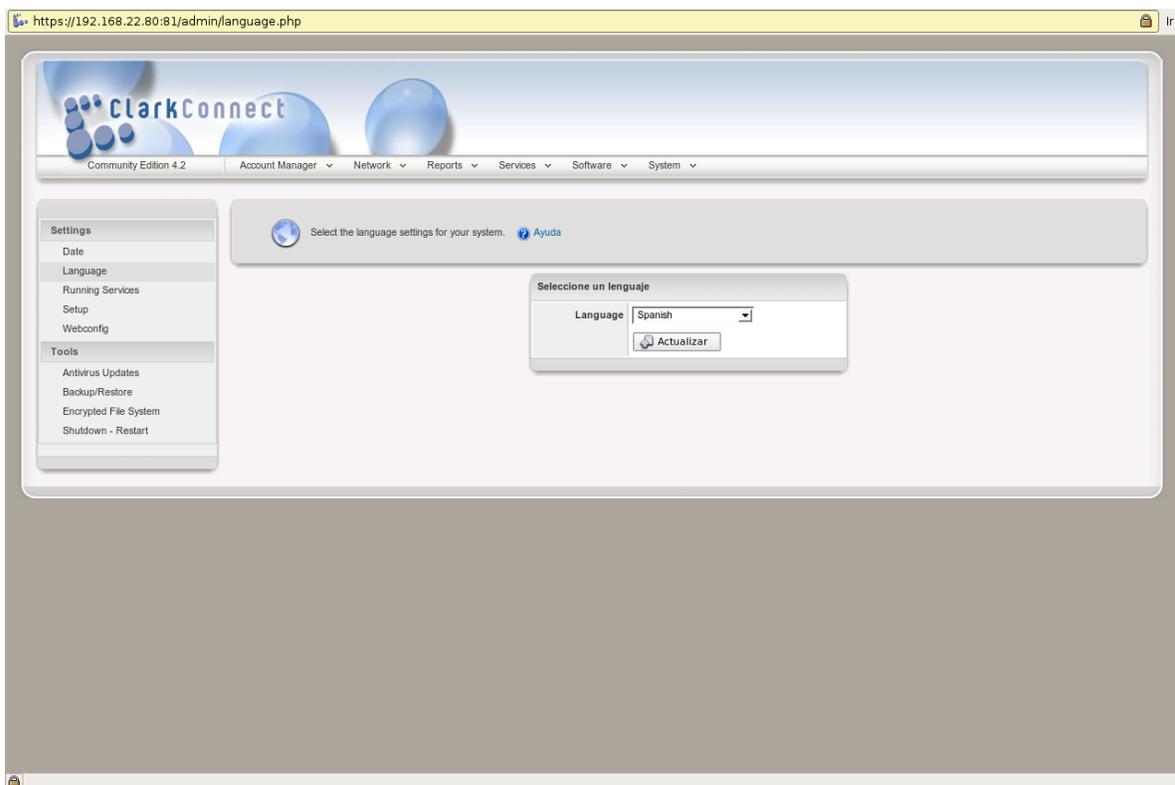


Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

La herramienta para la configuración de hora y fecha nos permite modificar la Zona Horaria para establecer una hora mas acorde con nuestra localización. Si se activa *Automatic Synchronize*, el servidor sincronizará su hora y fecha con respecto a servidores *NTP*<sup>54</sup> en Internet. Esto permitirá mantener una hora casi perfecta.

### 5.3.10.2 LENGUAJE

[Imagen sys2]



<sup>54</sup> *Network Time Protocol*, protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de Internet.

Aquí se puede cambiar el lenguaje por defecto que se usa en el *Webconfig*. Se recomienda seleccionar Inglés, ya que aun no existen traducciones completas al español.

### 5.3.10.3 SERVICIOS (Running Services)

[Imagen sys3]

Community Edition 4.2 Account Manager Network Reports Services Software System

Settings  
Date  
Language  
Running Services  
Setup  
Webconfig  
Tools  
Antivirus Updates  
Backup/Restore  
Encrypted File System  
Shutdown - Restart

Puede controlar el software ejecutándose en su sistema. Si desea que un servicio empiece automáticamente en un reinicio, asegúrese al inicio que la columna este en Automático. Algunos servicios tardan tiempo en iniciar/detener... sea paciente! Ayuda

Servicio	Estado	En Boot	
Antivirus Updates	Detenido	Manual	Configure
Content Filter	Detenido	Manual	Configure
DNS Cache	Ejecutándose	Automático	Configure
Intrusion Detection	Ejecutándose	Automático	Configure
Intrusion Prevention	Ejecutándose	Automático	Configure
Web Proxy	Ejecutándose	Automático	Configure

Servicio	Estado	En Boot	
Cron	Ejecutándose	Automático	Alto Al Manual
Logging Service	Ejecutándose	Automático	Alto Al Manual
SASL Authentication	Ejecutándose	Automático	Alto Al Manual
Secure Shell	Ejecutándose	Automático	Alto Al Manual
System Database	Ejecutándose	Automático	Alto Al Manual
System Watch	Ejecutándose	Automático	Alto Al Manual
User Database / LDAP	Ejecutándose	Automático	Alto Al Manual
User Database / Synchronize	Ejecutándose	Automático	Alto Al Manual
Web Services	Ejecutándose	Automático	Alto Al Manual

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

Esta página muestra en una excelente forma que servicios, procesos y demonios (*Daemons*) están corriendo y cuales se encuentran detenidos. El color verde simboliza que el proceso esta activado y el rojo lo contrario.

Si se quiere modificar el estado de un servicio (*Standard Services*) se debe presionar *Configure* y desde allí iniciarlo o detenerlo. Para los servicios del sistema o demonios (*Core Services*) desde esta misma página se puede modificar su estado.

Es conveniente revisar constantemente esta página para conocer el estado de los servicios y demonios.

Si se desea que el servicio se inicie cuando el sistema se inicia y no manualmente, la opción *Automatic* debe aparecer para dicho servicio, de lo contrario hay que modificarlo con los pasos arriba descritos.

Desde una consola con permisos de *root* también es posible controlar los servicios y demonios. Para hacer esto iniciamos sesión como *root* en una consola, bien sea local o remotamente, y escribimos:

```
/etc/init.d/[nombre_del_servicio] [opción]
```

Ejemplo: `/etc/init.d/squid restart`

Para saber como se llama un servicio o demonio podemos averiguarlo leyendo el enlace del *Webconfig* que lo configura:

```
https://192.168.1.254:81/admin/squid.php
```

O podemos ejecutar este comando el cual nos mostrara cuales son los servicios existentes en el servidor:

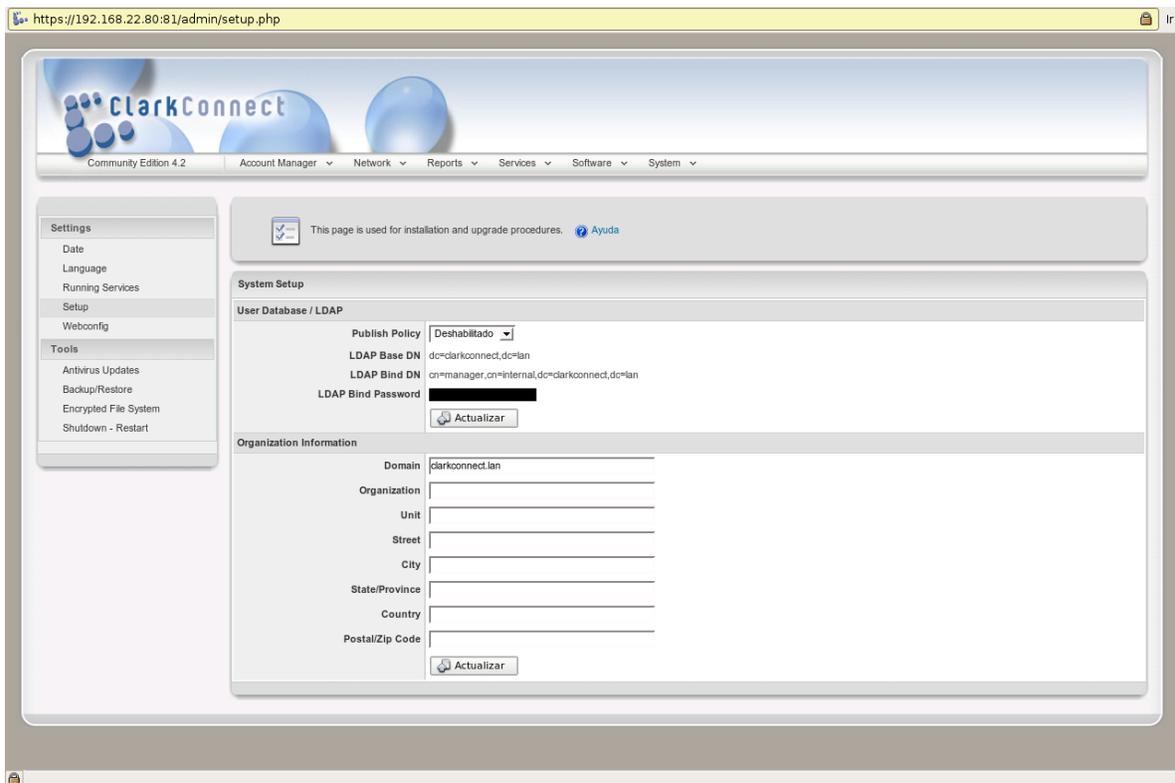
```
ls /etc/init.d/
```

Existen cuatro opciones importantes para manejar estos servicios:

1. *start*, inicia un servicio o demonio detenido.
2. *stop*, detiene el servicio especificado.
3. *restart*, reiniciar un servicio, primero lo detiene y luego lo inicia, es lo mismo que escribir *stop* y luego *start*.
4. *status*, muestra el estado del servicio, si se encuentra activo y corriendo o si esta detenido.

### 5.3.10.4 SETUP

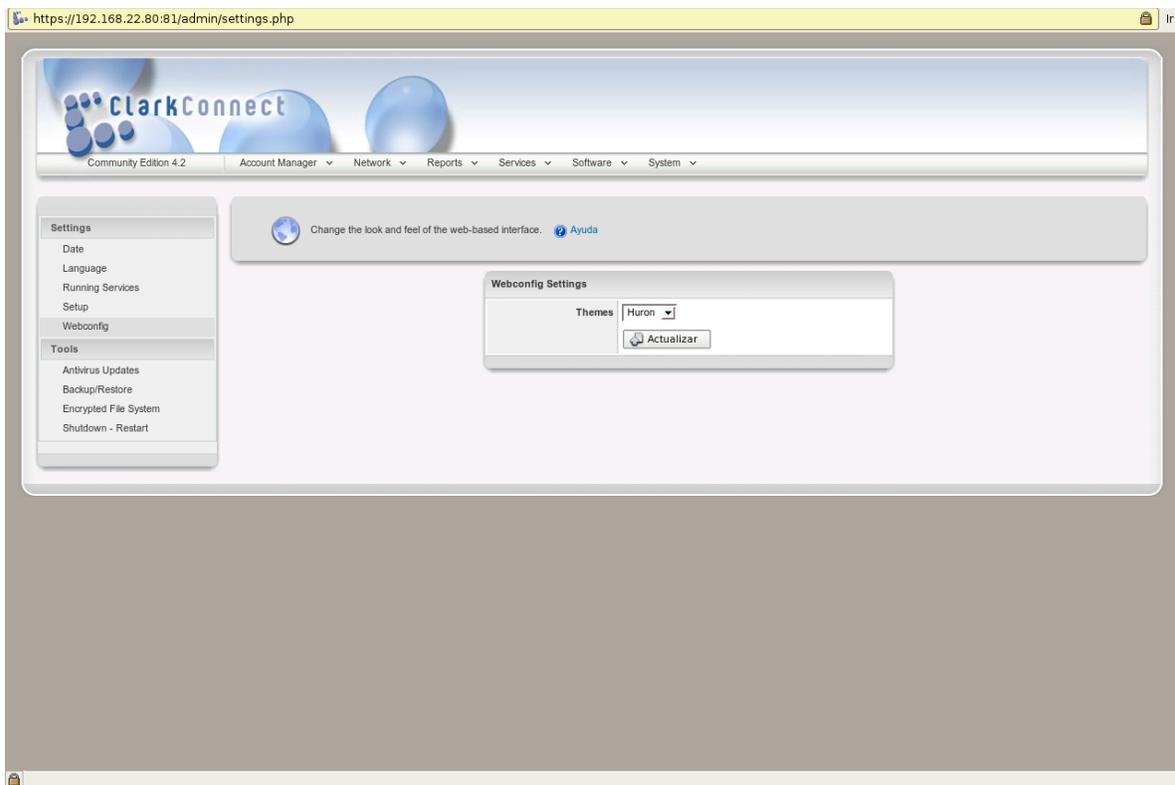
[Imagen sys4]



Esta sección es usado para procedimientos durante la instalación y una actualización del sistema. Si se desea se pueden escribir los datos de la organización como dominio del servidor, nombre de la organización, ciudad, y demás.

## 5.3.10.5 WEBCONFIG

[Imagen sys5]



Aquí se puede cambiar el aspecto visual del *Webconfig* para que se acomode a los gustos del administrador de la red, incluso si se desea se puede crear una plantilla propia, en este enlace explican como hacerlo:

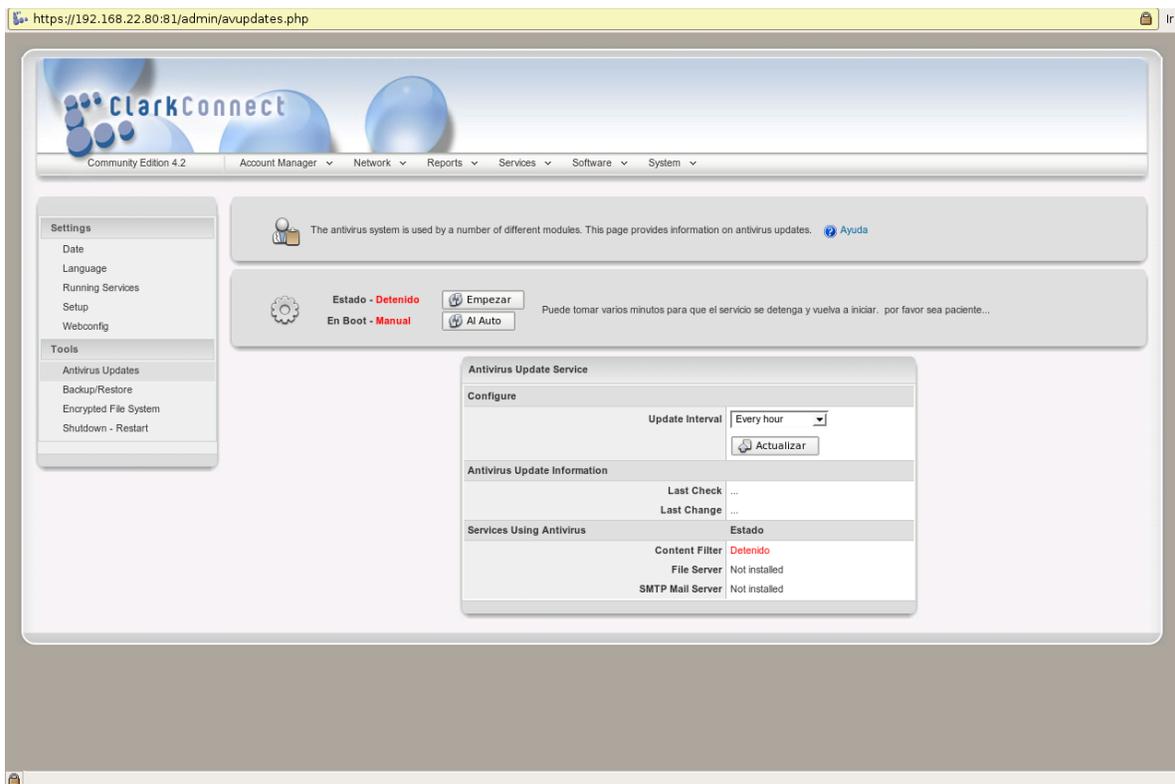
<http://www.ClarkConnect.com/developer/resources/webconfigskins.php>

## 5.3.11 SYSTEM TOOLS

En esta sección se reúnen algunas herramientas para la administración de los módulos y del sistema.

### 5.3.11.1 ACTUALIZACIONES DEL ANTIVIRUS

[Imagen sys6]



The screenshot shows the ClarkConnect web interface for managing antivirus updates. The browser address bar displays `https://192.168.22.80:81/admin/avupdates.php`. The interface includes a navigation menu with options like Account Manager, Network, Reports, Services, Software, and System. A left sidebar lists settings (Date, Language, Running Services, Setup, Webconfig) and tools (Antivirus Updates, Backup/Restore, Encrypted File System, Shutdown - Restart). The main content area features a status bar indicating the system is "Detenido" (Stopped) and "En Boot - Manual". It provides buttons to "Empezar" (Start) or "Al Auto" (Automatic). Below this, the "Antivirus Update Service" configuration is shown, with the "Update Interval" set to "Every hour" and an "Actualizar" (Update) button. The "Antivirus Update Information" section shows "Last Check" and "Last Change" as "...". The "Services Using Antivirus" table lists the status of various services:

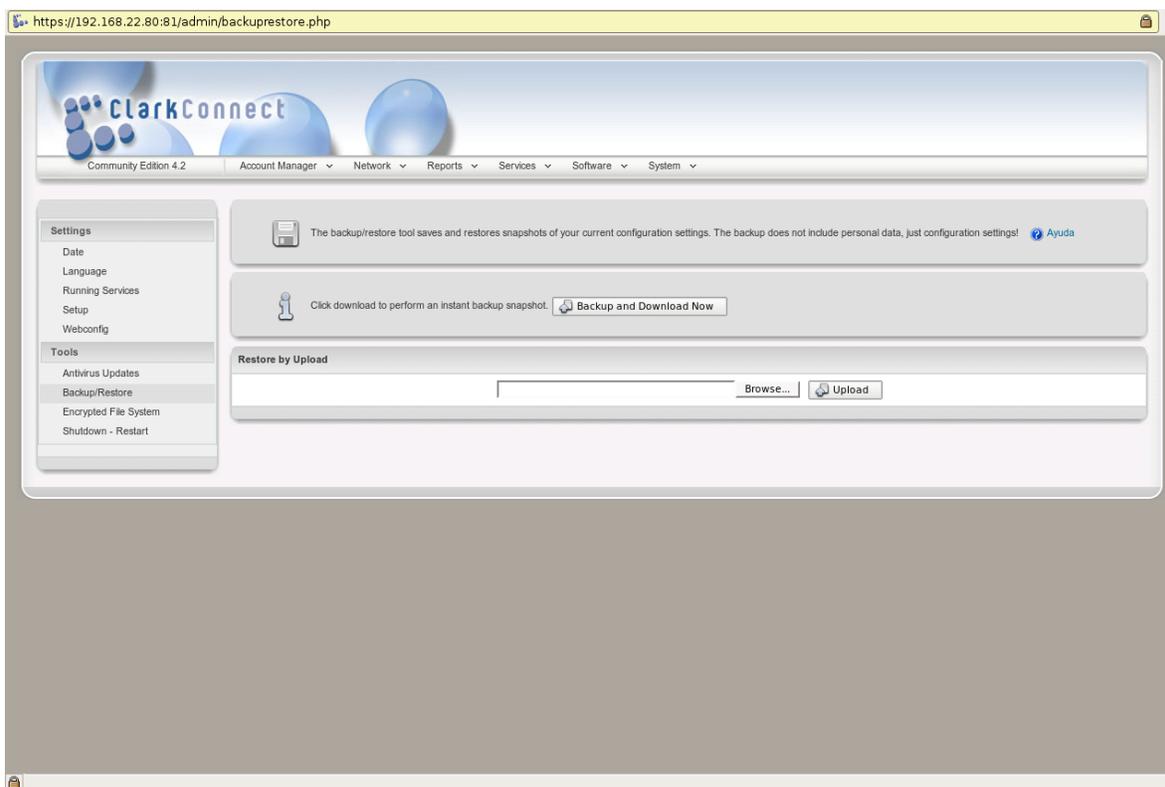
Services Using Antivirus	Estado
Content Filter	Detenido
File Server	Not installed
SMTP Mail Server	Not installed

Desde aquí se modifica el módulo de actualización del antivirus; se especifica con que periodicidad se debe actualizar automáticamente la base de datos del antivirus, cada hora, cada dos horas, dos veces al día o diariamente.

También se muestra información sobre los últimos cambios realizados a la base de firmas de virus y que otros módulos usan el antivirus, como el filtro de contenido o el servidor de correo.

### 5.3.11.2 COPIA DE SEGURIDAD/RESTAURACIÓN

[Imagen sys7]



Esta es una herramienta muy interesante porque permite realizar una copia de seguridad (*Backup*) de todos los archivos de configuración para una posterior restauración. Brinda adicionalmente la opción de almacenar esta copia en un sistema externo, por ejemplo otra máquina, un *CD-ROM*, un disco duro extraíble, en Internet, etc; brindando así mas redundancia a la copia de seguridad.

Si por alguna razón se necesita reinstalar el servidor, para volver al estado previo antes de la reinstalación y/o del daño ocurrido, solo basta con restaurar los archivos de configuración de la copia de seguridad.

Los archivos que son copiados y almacenados son únicamente archivos de configuración como los nombres de usuario y sus contraseñas, la configuración de la red, la configuración del *Firewall* y la configuración de algunos módulos de *software* como el filtro de contenido o el *Proxy*.

Para realizar un *Backup* presionamos el botón Backup and Download Now, y después de un momento podremos descargar el archivo `tar.gz`, el cual contiene los archivos empaquetados y comprimidos. La extensión `tar.gz` es una extensión de archivo que se usa para empaquetar y comprimir una carpeta o muchos archivos dentro de un solo archivo fácil de transportar. Es una extensión muy común en el mundo *Linux* y tiene soporte en cualquier distribución; adicionalmente existen programas *Windows*® y *MAC OS*® para extraer los archivos.

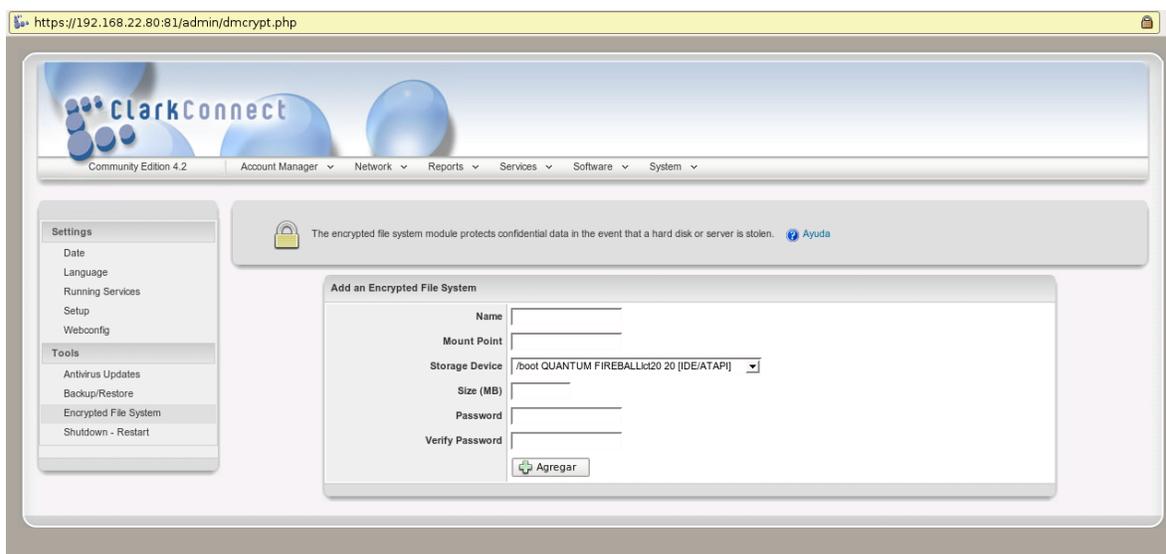
Para restaurar un *Backup* podemos realizar dos procedimientos:

1. A través de Examinar. . . : buscamos el archivo `tar.gz` que deseamos restaurar y presionamos Upload.

2. Conforme se van creando las copias de seguridad, una lista las muestra en orden cronológico, se pueden realizar las dos acciones que los botones indican, descargar nuevamente el *Backup* o restaurarlo según sea el caso.

### 5.3.11.3 ENCRYPTED FILE SYSTEM

[Imagen sys8]



Herramienta de seguridad que permite crear un volumen cifrado para proteger la información que se encuentra dentro, de acceso no autorizado o de robo. Esto le brinda mayor seguridad a la información

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar

sensible cuando no se encuentra en el servidor, por ejemplo cuando es transportada.

La protección solo se brinda a volúmenes que no se encuentran montados en el sistema, así cuando el servidor se encuentra encendido y funcionando esta seguridad basada en el cifrado no es aplicada.

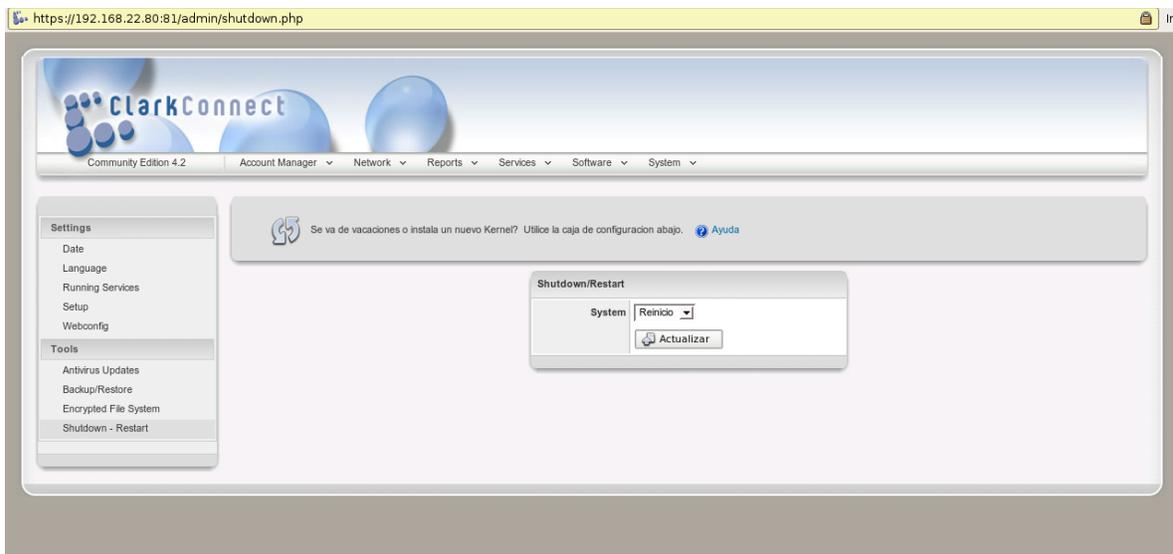
Pasos para crear un nuevo volumen:

1. Escoger un nombre para el volumen.
2. El punto de montaje es el lugar donde se montará el volumen, por defecto se ubica en `/mnt/dmccrypt/[nombre_volumen]`, pero aun así se puede cambiar el lugar como por ejemplo: `/root/Backup`, siendo *Backup* el nombre del volumen.
3. Aquí se escoge en cual disco o unidad se desea crear el volumen.
4. Se especifica el tamaño el volumen nuevo.
5. Finalmente se escribe la contraseña con la cual se protegerá el volumen.

¡Si por alguna razón se olvida la contraseña es imposible rescatar los datos que contenía el volumen!

### 5.3.11.4 SHUTDOWN - RESTART

[Imagen sys9]



Esta es la ultima herramienta de esta sección, nos da la posibilidad de apagar (Shutdown) o reiniciar (Restart) el sistema desde el *Webconfig*. Para realizar alguna de las dos acciones se escoge Shutdown o Restart del menú desplegable y se presiona *Update*, después el sistema preguntará si queremos realizar la acción seleccionada, presionamos en *Continue* y el servidor aceptará nuestra orden, y en cuestión de unos minutos finalizará.

Estas mismas acciones se pueden realizar desde una consola con

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar  
permisos de *root*, para apagar se ejecuta: `halt` y para reiniciar: `reboot`.

### **5.3.12 CONFIGURACIONES ADICIONALES**

En este momento el Servidor/*Firewall* debe estar corriendo y funcionando, ya se ha visto como se configuran las diferentes herramientas y módulos de *software*, se manejan las secciones de reportes para conocer del funcionamiento del *ClarkConnect*; ahora continuamos con otros módulos los cuales no son necesarios pero si interesantes y útiles para explorar.

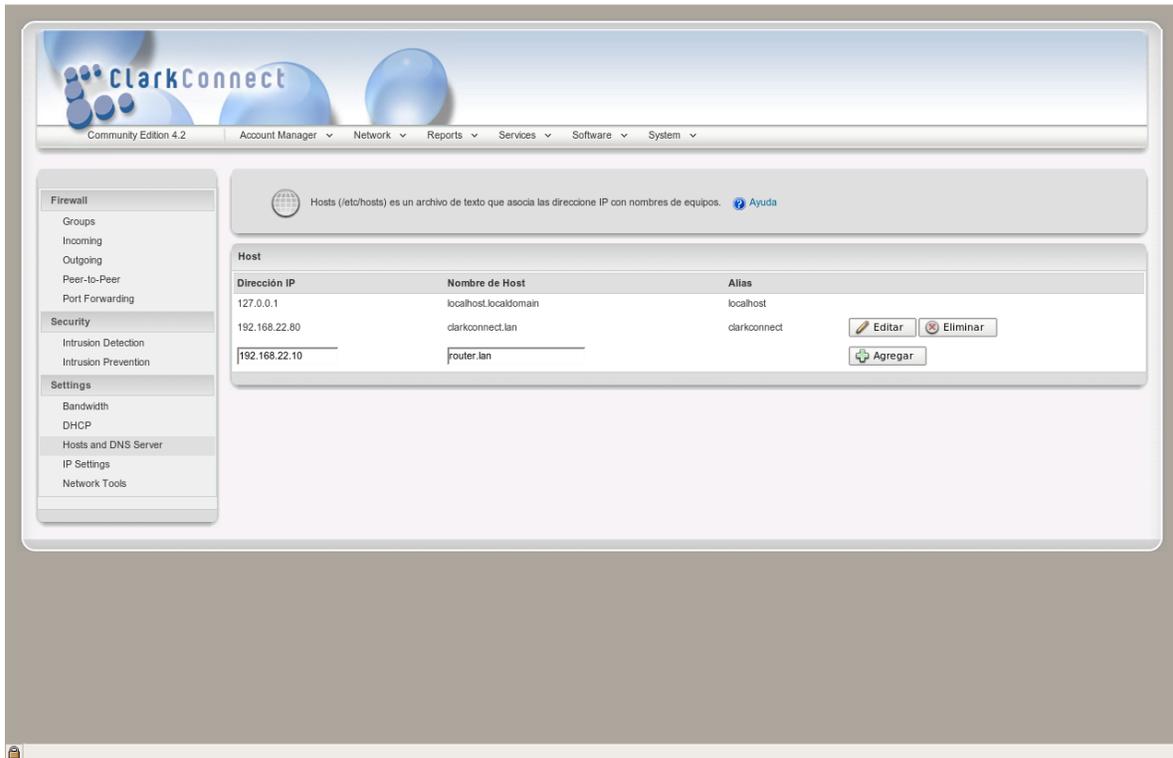
Aunque esta sección no es de lectura obligada se recomienda leerla.

### **5.3.12.1 HOSTS AND DNS SERVERS**

Este módulo en la sección de `Network Settings` nos permite configurar los alias para los *Hosts* en la configuración del servidor *DNS*. Esto ayuda a nombrar a un *Host*, el cual puede ser cualquier máquina, un servidor, un ruteador, una impresora o un dispositivo que se conecte a la red, con un alias el cual puede “reemplazar” la dirección de *IP* de este. Por ejemplo: el *Firewall* posee la *IP* `192.168.1.254` , pero a veces aprenderse este número no es sencillo, por eso el alias `clarkconnect.lan` es equivalente, si queremos acceder al servidor, podemos emplear cualquiera de los dos métodos y no hay problema.

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen net6]



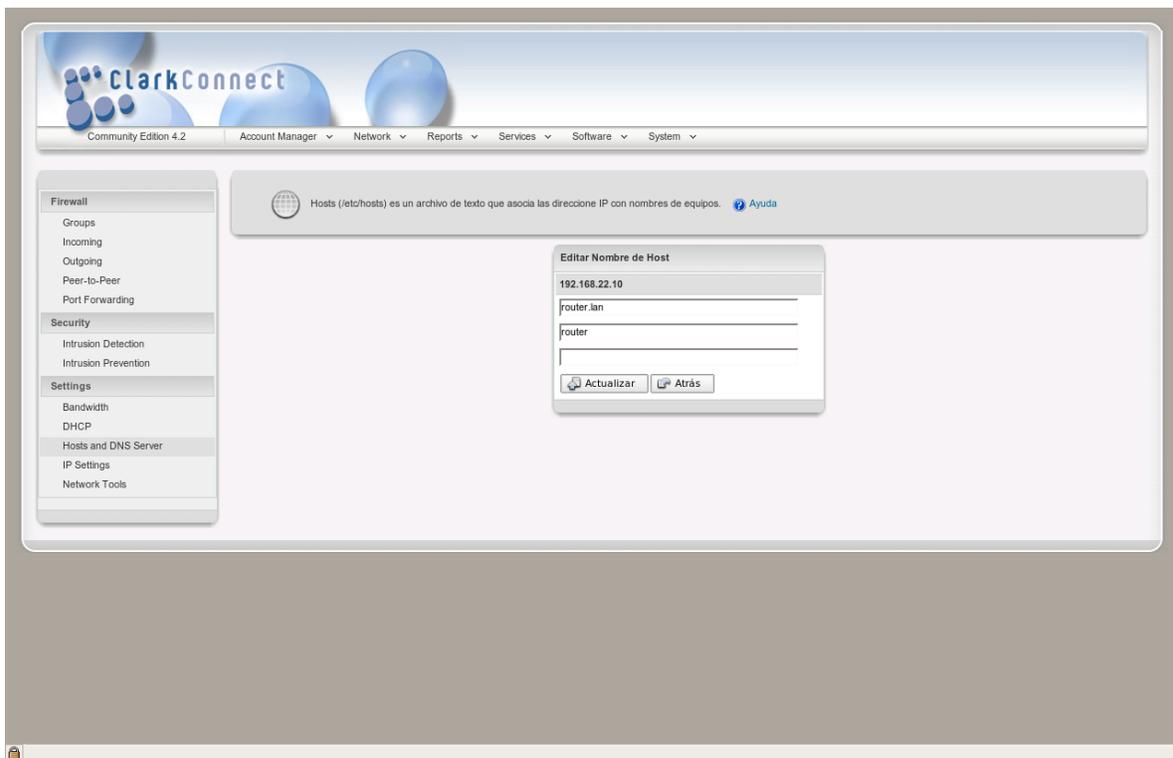
Para esto, el *ClarkConnect* funciona como un servidor *DNS*, el cual guarda en el archivo `/etc/hosts/` una lista donde por cada dirección de *IP* se asocia uno o varios alias que representan a esa dirección. Incluso si la máquina que realiza la petición pertenece al mismo dominio, en este caso `> .lan <` puede acceder a la máquina omitiendo ese fragmente de la dirección, ejemplo:

```
ping 192.168.22.80
ping clarkconnect.lan
ping ClarkConnect
```

Estos tres comandos y sus direcciones realizan lo mismo.

Para crear un nuevo alias, se ingresa a la sección Hosts and DNS Server en Network. En la página se ve una lista con tres datos importantes y los botones para realizar las acciones. Primero se la dirección de IP del Host, seguido el nombre del Host (*Hosts Name*) que se emplea para identificarla y finalmente el o los alias que se pueden usar en reemplazo de la dirección de IP. Para cada Host se pueden emplear diferentes alias.

[Imagen net7]



En la sección inferior se encuentran dos cuadros de texto, en el primero

Implementación de un Servidor/*Firewall GNU/Linux* en un entorno escolar se ingresa la dirección de *IP* del *Host* y en el segundo el nombre del *Host* que se le va a dar, ejemplo:

```
192.168.1.250  router1.lan
```

### **5.3.12.2 NETWORK TOOLS**

Este módulo cuenta con tres herramientas para monitorizar y diagnosticar la red, en tres aspectos: información en tiempo real de las conexiones actuales; información sobre la ruta de las paquetes de red y estadísticas sobre los protocolos de red.

## [Imagen net8]

The screenshot displays the Mikrotik WinBox interface for the Connection Monitor tool. The browser address bar shows `https://192.168.22.80:81/admin/nettools.php`. The interface includes a navigation menu on the left with categories like Firewall, Security, and Settings. The main content area features a 'Network Tools' section with a dropdown menu set to 'Connection Monitor' and a 'Generar' button. Below this is a 'Connection Monitor' control panel with a 'Refresh' input set to '0' and an 'Actualizar' button. The central part of the interface is a table titled 'Connection Count - 15' with the following columns: Protocolo, Expires, Source, Destination, Estado, Puerto, and Servicio. The table lists various active connections, including TCP and UDP sessions from external sources to internal LAN addresses. A color-coded bar at the bottom of the table identifies the source and destination zones: Internet (red), External (orange), DMZ (yellow), LAN (green), and Loopback (black).

Protocolo	Expires	Source	Destination	Estado	Puerto	Servicio
TCP	01:11:06.72	127.0.0.1	127.0.0.1	ESTABLISHED	3568->9999	
UDP	00:00:00.28	10.80.0.1	255.255.255.255		67->68	BOOTPC
TCP	01:11:59.99	192.168.22.107	192.168.22.80	ESTABLISHED	54542->81	
TCP	01:11:59.93	192.168.22.107	[REDACTED]	ESTABLISHED	42148->5190	
UDP	00:00:00.20	PUBLIC*	[REDACTED]		1035->53	DOMAIN
TCP	01:11:29.45	127.0.0.1	127.0.0.1	ESTABLISHED	3530->1903	
TCP	01:11:29.45	127.0.0.1	127.0.0.1	ESTABLISHED	3234->4107	
UDP	00:00:01.70	PUBLIC*	[REDACTED]		1035->53	DOMAIN
TCP	00:00:00.09	192.168.22.107	192.168.22.80	CLOSE	54541->81	
TCP	01:11:29.45	127.0.0.1	127.0.0.1	ESTABLISHED	4609->2499	
TCP	01:10:50.58	192.168.22.107	192.168.22.80	ESTABLISHED	59305->22	SSH
TCP	01:11:59.99	192.168.22.107	192.168.22.80	ESTABLISHED	54543->81	
TCP	01:11:57.55	192.168.22.107	[REDACTED]	ESTABLISHED	38438->5190	
TCP	01:11:29.45	127.0.0.1	127.0.0.1	ESTABLISHED	1193->3382	
TCP	01:11:59.95	192.168.22.107	[REDACTED]	ESTABLISHED	39288->1863	

1. Connection Monitor, herramienta que muestra información en tiempo real de las conexiones que pasan a través del *Firewall*. Puede ser útil para identificar conexiones abiertas creadas por *Malware*, aplicaciones *P2P* o para saber que causa problemas en la red. Se muestran siete columnas, cada una contiene datos de cada conexión existente:

- El protocolo de la conexión; *TCP/UDP*.
- El tiempo restante para que la conexión expire.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

- La fuente de donde proviene la conexión, una dirección de *IP* que identifica al *Host* por medio de cinco colores: rojo, Internet; naranja, la *IP* pública del servidor; amarillo, *DMZ*; verde, red local; negro, interfaz local o *loopback* (usado comúnmente por servicios y demonios).
- El destino, dirección de *IP* a cual es dirigida la conexión, el mismo código de colores descrito anteriormente es usado aquí.
- El estado: establecido, cerrado, escuchando, (*Established, Close, Listening*).
- Puerto usado por la conexiones, el primero indica de donde provienen y el segundo a donde se dirige.
- Servicio asociado a la conexión, si es conocido.

Al presionar en `update` se puede actualizar la información aquí mostrada, si se escribe un número reemplazando al cero `>0<`, este es el número de segundos que pasan antes de actualizar automáticamente la página.

2. `Routing Table`, la tabla de “enrutamiento” que representa el camino que debe seguir un paquete para llegar a la red de destino. Se muestran ocho columnas, pero para nuestro caso solo cinco son necesarias; para que un paquete llegue a la red de destino (columna 1) con una máscara de red (columna 3), debe pasar por la puerta de enlace o *gateway* (columna 2) usando el adaptador de red (columna 8). La columna 5 muestra el número de saltos que debe realizar el paquete al pasar por los nodos, usualmente “ruteadores”, para llegar a su destino.

3. *Protocol Statistics*, muestra información técnica sobre los protocolos usados en la red, como: *ICMP*, *TCP* y *UDP*.

### **5.3.12.3 ACCESS CONTROL (CONTROL DE ACCESO)**

El control de acceso puede ser usado para permitir o denegar el acceso a Internet, para navegar a través del *Proxy*, a ciertas horas del día o días de las semana, a un grupo de usuarios. Su configuración es sencilla y puede ayudar a mejorar la política institucional en cuestión para la navegación en Internet. Puede ser usado de igual forma para mejorar la seguridad de la red e impedir que otros usuarios naveguen a través del *Proxy* en horarios no aprobados.

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

[Imagen soft8]

The screenshot displays the ClarkConnect web interface. The browser address bar shows the URL `https://192.168.22.80:81/admin/squidacl.php`. The interface features a header with the ClarkConnect logo and navigation menus for Account Manager, Network, Reports, Services, Software, and System. A left sidebar lists options: Proxy and Filtering, Access Control, Content Filter, and Web Proxy. The main content area includes a section for Time-based Access Control with a description and an 'Ayuda' link. Below this is a 'Time-Based Access Control' section with tabs for 'Access Control Lists', 'Add/Edit Access Control', and 'Add/Edit Time Periods'. A table with columns 'Name', 'ACL Type', 'Time-of-Day ACL', 'User/IP/MAC', and 'Priority' is shown, containing the text 'No records found.'

## **CAPÍTULO 6**

### **6.1 COMANDOS DE ADMINISTRACIÓN DEL SERVIDOR**

En este nuevo capítulo vamos a ver trucos y comandos enfocados y estructurados en diferentes aspectos para simplificar el trabajo de administrar un servidor *GNU/Linux* y así maximizar el uso del tiempo.

Se recomienda ejecutar en la consola el comando `man` seguido del nombre del comando (`man [nombre_comando]`), para conocer el manual y la información referente al segundo. Esta es una gran fuente de información para comenzar a conocer el sistema y a los comandos. No todos poseen un manual pero la gran mayoría lo tienen, si se desea conocer con mayor profundidad o con otro punto de vista se puede buscar en internet.

## 6.2 MONITOREO REMOTO DE SERVIDORES

Realizar un monitoreo periódico a un Servidor, y más si es un *Firewall*, es una de las responsabilidades que el administrador de la red tiene, y debe hacerlo continuamente para garantizar que la máquina trabaje apropiadamente y no hayan huecos de seguridad u otras fallas que puedan impedir el correcto funcionamiento. Al ser una máquina que se encuentra entre dos redes, siendo una de ellas el internet, el *Firewall* es un objetivo constante de muchas amenazas, saber que sucede y estar atento es importante para garantizar protección a toda la red. El monitoreo se realiza con el objetivo de obtener información en tiempo real para diagnosticar al Servidor y buscar posibles o futuros problemas. Como administrador se debe saber que ocurre a cada instante en el Servidor, como el porcentaje de recursos (memoria, procesador, disco duro) gastados, o el tráfico de la red.

El monitoreo se centra en cuatro aspectos importantes: el procesador, la memoria, el disco duro y el estado de la red.

**Nota:** Como se explicó anteriormente (apartado 5.3.5) podemos acceder al *ClarkConnect* por medio del protocolo *SSH* y evitar estar presentes físicamente en el *Firewall* al momento de realizar el monitoreo.

A continuación se listan los comandos a ejecutar:

- `hostname`, se utiliza para mostrar o establecer el nombre actual del sistema. Con este comando nos aseguramos que estemos en la máquina correcta al realizar el monitoreo.
- `date`, informa de la hora local del sistema. Se usa para verificar la fecha y mantener los *logs* con la hora correcta. Un atacante podría cambiar la fecha y así engañar al administrador con respecto a la verdadera hora del suceso.
- `top`, nos muestra los recursos del sistema utilizados mientras se corre el comando, esto puede ser útil para saber de una forma general, actual y resumida que porcentaje del procesador es usado, cuanta memoria es usada y cuales son los procesos mas usados por el sistema. Actualmente existe un mejor comando que *top*, `htop` ([htop.sourceforge.net](http://htop.sourceforge.net)), este muestra de una forma mas colorida la información, con la posibilidad de modificar el modo de presentarla en pantalla.
- `less /proc/cpuinfo`, información del procesador como nombre, velocidad, cache, etc.
- `less /proc/meminfo`, información de la memoria *RAM*, muestra la cantidad total, la disponible y la usada al igual que otras variables, este archivo es útil para conocer como se distribuyen los procesos en la memoria, y puede servir como un primer diagnostico si se tienen problemas de memoria.

## Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

- `free`, información de la memoria física y de intercambio en el sistema. La columna de memoria compartida debe ignorarse ya que es obsoleta.
- `ps`, muestra una instantánea de los procesos actuales que corren en el sistema. Adicionalmente incluye información importante sobre el proceso como: el usuario que lo ejecuta, el *PID* o el número de proceso que tiene, la carga que le genera al procesador, cuanto gasta en memoria, la hora de inicio y el nombre del proceso.
- `apt-get`, comando y herramienta usado para la administración de paquetes. Este comando usa varios argumentos al momento de ejecutarse para realizar diferentes procedimientos, pero para esta sección solo usaremos tres argumentos: *update*, *upgrade* y *dist-upgrade* . Estos actualizan la base de datos de los paquetes de *software*, actualizan inteligentemente el *software* instalado y actualizan el *software* a una versión mayor por ejemplo de 4.1 a 4.2, respectivamente.
- `df`, muestra la cantidad de espacio de disco usado y la disponible en los sistemas de ficheros de la máquina.
- `du`, muestra la cantidad de espacio de disco usado por los archivos especificados. Se usa también para conocer cuanto espacio ocupa la jerarquía de archivos especificada, ejemplo: para conocer

cuanto espacio de disco ocupa un usuario específico se escribe:  
`df -h /home/usuario .`

- `/etc/init.d/clamd status`, comprueba el estado del antivirus del sistema, el *Clamd*. Si todo sale bien la respuesta es positiva e indica el *PID* del proceso, de lo contrario nos avisará que algo está mal; para iniciar el *Clamd* se ejecuta: `/etc/init.d/clamd start .`

#### **Lista de comandos:**

1. `hostname`
2. `date`
3. `top`
4. `less /proc/cpuinfo`
5. `less /proc/meminfo`
6. `free -m`
7. `ps auxw`
8. `apt-get [update; upgrade; dist-upgrade]`
9. `df -h`
10. `du -h [directorio]`
11. `/etc/init.d/clamd status`

## **6.3 COMANDOS DE ADMINISTRACIÓN BÁSICA**

Las tareas de administración del sistema son principalmente garantizar el correcto funcionamiento de todos los componentes, de allí el nombre sistema, un conjunto o grupo de componentes u objetos que trabajan juntos en un entorno o con un fin, en este caso formar una máquina, en concreto un *Firewall*.

Configurar y administrar un sistema es una tarea bastante compleja, la cual esta fuera de límites de este trabajo (existen textos, libros y mas material sobre este tema), más aún no podemos dejarla a un lado, por eso explicaré brevemente algunos comandos y procesos que se deben de llevar a cabo para la administración básica de un servidor *Linux*.

Todos los comandos que siguen a continuación se deben ejecutar como *root* o superusuario, de lo contrario no funcionarán. Es necesario ser cauteloso y leer atentamente para evitar posibles errores, los cuales no tengan arreglo.

- `nano55 /etc/issue` , modifica el mensaje de entrada de la consola, por ejemplo para advertir a un desconocido o para cambiar el texto que se muestra.

---

<sup>55</sup> Programa por consola para la edición de texto de cualquier archivo de texto plano.

- `nano /etc/motd` , este es el mensaje que se muestra al usuario después de iniciar sesión (por consola) exitosamente. Normalmente contiene un breve texto referente al sistema o un mensaje a los usuarios.
- `/usr/sbin/kudzu` , ejecuta la herramienta de *Red Hat Linux* para la configuración de *hardware*. Esta se ejecuta durante el inicio del sistema para verificar si algún *hardware* fue removido o instalado en la máquina. Normalmente no es necesario ejecutarlo, pero puede ser conveniente para revisar la configuración del *hardware*.
- `passwd` , cambia las contraseñas en el sistema. Si este comando es usado sólo cambiará la contraseña del usuario que lo está corriendo, para cambiar la contraseña de otro usuario se debe ejecutar: `passwd [nombre_usuario]`
- `lastlog` , muestra una lista de todos los usuarios y a su vez la fecha, hora y puerto de consola por el cuál ingresaron la última vez en el sistema.
- `who` , despliega en pantalla la lista de los usuarios conectados actualmente en el sistema. Es conveniente revisar que no existan usuarios no autorizados conectados.
- `ps tree | less` , estos son dos comandos, de los cuales la salida del primero se concatena con el segundo para un mejor análisis de

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

la información. Al ejecutar `ps tree` despliega un árbol con los comandos ejecutándose actualmente en el sistema y muestra quien es el padre del comando o de donde provino la orden de ejecutarse.

- `kill` , manda una señal a un proceso, usualmente es la señal **TERM** la cual es usada para terminar (matar) al proceso. Para su uso se debe conocer el *PID* del proceso el cual aparece con el comando `ps` .
- `last` , este comando es mas especial que `lastlog` y mucho mas poderoso aunque su función sea simplemente leer un archivo de *log*. `last` despliega un listado de los últimos usuarios conectados junto con otra información como la fecha de ingreso, el tiempo de la sesión y la consola de ingreso, adicionalmente es útil para conocer cuando fue reiniciado o apagado el sistema sin nuestro consentimiento, para esto hay que ejecutar `last reboot` .
- `/sbin/shutdown` , este es el comando usado para cerrar, reiniciar o apagar el sistema de un modo seguro y sin perdida de información. Si se desea se puede especificar una hora determinada para el apagado del sistema. Cuando se ejecuta este comando manda un aviso de advertencia a todos los usuarios y procesos. Opciones del comando:
  - `-r` reinicia el sistema
  - `-h` apaga el sistema

- `-c` detiene una secuencia de apagado

Ejemplo: `/sbin/shutdown -h 23:00` el sistema se apagará a las  
23 horas locales.

- `halt` y `reboot`, son variantes del comando `shutdown` y su uso es similar, solo basta con escribir y ejecutar. ¡Este comando no se puede configurar para ejecutarse a una hora predefinida!

#### **Lista de comandos:**

1. `nano /etc/issue`
2. `nano /etc/motd`
3. `/usr/sbin/kudzu`
4. `passwd [usuario]`
5. `lastlog`
6. `who`
7. `pstree | less`
8. `kill [PID]`
9. `last`
10. `/sbin/shutdown -h [hora]`

## 6.4 MONTAR MEDIOS DE ALMACENAMIENTO (`mount`)

Montar un sistema de ficheros (un disco duro, una partición, un *CD-ROM*) es una de las tareas mas importantes que realiza el SO al iniciar el sistema. En *Linux* este proceso se conoce con el nombre de *montaje*, y consta de añadir a la jerarquía de ficheros (*/*) el nuevo sistema de archivos. “Montar un sistema de ficheros no significa más que asociar un determinado nombre de directorio, denominado `mount point` o punto de montaje, con el sistema en cuestión, de forma que al utilizar dicha ruta estaremos trabajando sobre el sistema de ficheros que hemos asociado a ella.<sup>56</sup>”

El comando para montar es: `mount` , para ejecutarlo necesitamos conocer tres datos importantes:

- el nombre y tipo de dispositivo que vamos a montar
- el sitio o destino, desde el cual se montará el nuevo sistema de ficheros
- el tipo o formato del medio de almacenamiento

Ejemplos: `mount -t ntfs-3g /dev/sda1 /mnt/sda1`

`mount -t ext3 /dev/sdb1 /home/admin/backup`

---

<sup>56</sup> Cita de <http://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node54.html> por

## **6.5 PERMISOS DE USUARIOS Y DE ARCHIVOS - SEGURIDAD ELEMENTAL**

En *GNU/Linux* cada archivo tiene permisos, esto define quien puede ejecutarlo, escribirlo o leerlo. Esto se considera la seguridad mas básica y elemental en el SO. Los permisos de un archivo o directorio se reparten en tres características: *r* → lectura ; *w* → escritura y *x* → ejecución. Adicionalmente, se define quien puede acceder a los archivos de esta manera: propietario (*owner*), grupo (*group*) y otros (*other*). Todo eso para permitir o denegar el acceso a un archivo a los diferentes usuarios del SO. Este sistema permite una fácil gestión de los archivos y mantener una buena política de seguridad permite mejorar la confiabilidad del sistema.

Si ejecutamos el comando `ls -l` :

```
drwxr-xr-x  1 root root      4096 jul 03 23: 18 Prueba1
-rw-r--r--  1 root root    16488 jun 30 10: 37 Prueba2.txt
```

`ls` "escribe en formato de una sola columna los permisos del fichero, el número de enlaces que tiene, el nombre del propietario, el del grupo al que pertenece, el tamaño (en *bytes*), una marca de tiempo de la ultima modificación, y el nombre del fichero<sup>57</sup>".

---

<sup>57</sup>Cita de la página man del comando `ls`.

El primer *bit* de los permisos de fichero muestra también que tipo de archivo es: *d* para carpeta, *-* para archivo normal y *l* para enlace.

Los nueve *bits* restantes de la primera columna se agrupan en tríos para darle los permisos a los propietarios, grupos y otros.

En el primer ejemplo vemos que `Prueba1` es un directorio o carpeta, para el cual el propietario tiene todos los permisos (lectura, escritura y ejecución), y el grupo al cual pertenece el propietario y los otros usuarios tienen sólo los permisos de lectura y ejecución. “El carácter *-* indica la falta de ese derecho de acceso o permiso<sup>58</sup>”.

Es importante aprender el funcionamiento de los permisos de archivo ya que una buena política de permisos garantiza mayor seguridad del sistema.

### 6.5.1 MANEJO DE PERMISOS CON `chmod`

El comando `chmod` nos permite modificar los permisos de usuario, este comando es importante saber usarlo, se recomienda leer el manual del comando ejecutando: `man chmod`.

El uso del comando es simple y sencillo, primero se escribe el comando, las opciones (estas son opcionales), los permisos a modificar y

---

<sup>58</sup> Cita de Linux, administración del sistema y la red, página 40

finalmente el o los archivos a modificar. Ejemplo:

```
chmod g+w Prueba1
chmod 775 Prueba1
```

Estos dos ejemplos son equivalentes y hacen lo mismo, darle al grupo el permiso de escritura (*write*). Quedando finalmente con estos permisos:

```
drwxrwxr-x 1 root root 4096 jul 3 23:18 Prueba1
```

Los dos modos usados se llaman absoluto y relativo.

“El modo relativo permite añadir o eliminar permisos sobre los ya establecidos. Se suelen usar tres caracteres para este modo:

- el primero, para referirse al propietario, grupo o resto (otros) será *u* (*user*), *g* (*group*) y *o* (*others*). También se puede usar *a* para referirse a todos a la vez.
- El segundo será *+* para añadir el permiso o *-* para eliminarlo.
- El último será el propio permiso representado por el carácter *r*, *w* o *x*.

Por ejemplo, para añadir permiso de modificación al grupo se especificará *g+w*, mientras que para quitar el de ejecución al resto de cuentas se escribirá *o-x*.<sup>59</sup>”

---

<sup>59</sup> Cita de Linux, administración del sistema y la red, página 40

En el modo absoluto los permisos se establecen de otra forma, seleccionando los nueve *bits* de una sola vez. Con esto me refiero a los tres tríos de permisos que tiene cada archivo. Para ello se especifica en tres dígitos, el primero para el propietario, el segundo para el grupo y el tercero para los otros. Estos dígitos van desde el 0 hasta el 7, ya que cada permiso tiene un valor:

- el permiso de escritura (*read*) vale 4
- el permiso de lectura (*write*) vale 2, y
- el permiso de ejecución (*execution*) vale 1

4=r ; 2=w ; 1=x

Para asignar los permisos a cada usuario hay que combinar estos tres números, si queremos todos los permisos sumamos  $4+2+1=7$ , y ese es el número que debemos escribir; en cambio si deseamos solo permiso de lectura solo debemos escribir 4. Si no se quieren dar permisos se escribe 0. Ejemplo:

```
chmod 740 Prueba2.txt
```

Estos permisos le dan completo control al propietario, permite que el los usuarios que pertenezcan al grupo del propietario sólo puedan leer el archivo y finalmente deniega cualquier acceso al resto de los usuarios (*others*).

Si se desea cambiar todos los permisos de todos los archivos que cuelgan de un directorio de debe especificar como opción *-R*, ejemplo:

```
chmod -R a+r /home/user/*
```

## 6.5.2 CAMBIO DE PROPIETARIO Y DE GRUPO

Normalmente las tareas de administración se realizan siendo *root* los archivos creados por él sólo podrán ser ejecutados por él y ningún otro usuario a menos que pertenezcan al mismo grupo (pero esto se evita por seguridad).

Para evitarse este problema hay dos soluciones, ambas sencillas y con el poder de combinarlas:

*chown* nos permite cambiar de propietario, mientras que *chgrp* nos permite cambiar el grupo al cual pertenece el propietario.

Estos dos comandos son fáciles de usar y tienen sintaxis similar a *chmod*.

```
chown [opciones] usuario fichero1 fichero2 . . .
```

```
chown admin Prueba1
```

```
chown -R admin /home/user/*
```

El primer ejemplo cambia el propietario del archivo `Prueba1`. El segundo ejemplo cambia el propietario de todo el árbol de archivos que cuelga de `/home/user/*`.

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

```
chgrp [opciones] grupo fichero1 fichero2. . .  
chgrp usuarios Prueba2.txt  
chgrp -R admin /home/user/*
```

Estos dos ejemplos cambian el grupo del archivo y del árbol de archivos especificados.

## **6.6 CONFIGURACIÓN DE RED**

La configuración de la red es un trabajo que *ClarkConnect* nos soluciona desde el principio, pero a veces esta configuración no surte efecto o tenemos que realizar algunas correcciones y para esto tenemos que manipular algunos archivos de configuración y ejecutar unos cuantos comandos, no todos son para realizar cambios, también están otros para realizar diagnósticos o pruebas para conocer el estado de la red, para así aplicar los cambios necesarios para estar siempre en constante mejora.

## 6.6.1 ifconfig - EL COMANDO DE LAS INTERFACES

Este comando es muy versátil y permite realizar no solo configuraciones a las interfaces de red sino también conocer su actual configuración. Comenzaremos inicialmente con ejecutarlo solo: *ifconfig*, lo cual nos despliega una lista con todas las interfaces disponibles en el SO, junto con información asociada a cada una de ellas:

```
eth0      Link encap:Ethernet  HWaddr 00:1a:92:0b:ba:00
          inet addr:192.168.22.107  Bcast:192.168.22.255
          Mask:255.255.255.0
          inet6 addr: fe80::21a:92ff:fe0b:ca77/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3464 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2349864 (2.2 MiB)  TX bytes:1454729 (1.3 MiB)
          Interrupt:18 Base address:0x8000
```

- Link encap: tipo de interfaz, en este caso *Ethernet*
- Hwaddr: la dirección *MAC* de la tarjeta de red
- inet addr: dirección *IP* de la interfaz
- Bcast: dirección de *Broadcast*
- Mask: máscara de red

Esta es la información más importante que podemos obtener al ejecutar

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar

el comando sin ninguna opción. Si deseamos conocer esta misma información pero de una interfaz determinada simplemente se escribe el nombre de dicha interfaz detrás del comando como una opción, ejemplo: `ifconfig eth0` , este comando despliega la información disponible de la interfaz `eth0`.

Opciones de ejecución con el comando `ifconfig`:

- `ifconfig`: despliega información de todas las interfaces disponibles
- `ifconfig eth0`: despliega información de la interfaz especificada.
- `ifconfig eth0 up`: activa la interfaz especificada en la primera posición.
- `ifconfig eth0 down`: desactiva la interfaz especificada.
- `ifconfig eth0 192.168.0.1 netmask 255.255.255.0`: asigna la dirección de *IP* junto con la máscara de red a la interfaz especificada.

## 6.6.2 DNS - /etc/resolv.conf

Este archivo contiene unas cuantas líneas de texto con el dominio y las direcciones (de *IP*) de los servidores *DNS* a los que debe realizar peticiones la interfaz de red. Este archivo se puede editar con cualquier editor de texto plan como `nano` o `vim`.

Un ejemplo de la vista de este archivo de configuración es esta:

```
domain instituto.com
search instituto.com
nameserver 192.168.0.250
nameserver 192.168.0.251
```

La línea `domain` contiene el dominio de la red en la que se encuentra la máquina, la línea `search` indica buscar en ese dominio. Las líneas `nameserver` (que pueden ser varias) listan los servidores *DNS* a los cuales dirigir las peticiones de resolución de nombres, normalmente se escriben dos para tener mas redundancia con el servicio de *DNS*.

**Nota:** editar esta archivo de configuración puede causar problemas en la red, tener cuidado al hacerlo, es recomendable hacer una copia antes de editarlo.

### **6.6.3 dhclient - *Dynamic Host Configuration Protocol Client***

Comando para la configuración del protocolo *DHCP* en el cliente. Este comando se encarga de mandar una petición para que el servidor *DHCP* encargado le responda con la configuración necesaria para la red en la que se encuentra. Si se especifica una interfaz a esta se le asignará la nueva configuración.

### **6.6.4 ping - EL SONAR DE LA RED**

“Con el comando `ping` se comprueban las características actuales de la conexión de nuestro computador con otro computador en red o una subred concreta. La información que proporciona es doble: por un lado, comprueba si la conexión se puede establecer o no, y por otro lado mide la velocidad de transmisión (de cada paquete y la velocidad media de todos los paquetes enviados)”<sup>60</sup>.

Su uso es sencillo, se usa un único parámetro, el cual es una dirección (de IP) de una máquina en una red.

---

<sup>60</sup> Cita de Linux, administración del sistema y la red, página 171

Ejemplo:

```
ping 192.168.0.254  
ping google.com
```

El comando comienza a ejecutarse y a enviar paquetes *ICMP* en la dirección especificada esperando una respuesta y presentando los datos; para detener el comando se tecléa: *CRTL +C* .

Adicionalmente el comando puede ser usado para detectar el funcionamiento de varias máquinas en una red por medio de la opción de difusión o *broadcast*: *ping -b 192.168.0.255* .

### **6.6.5 traceroute - REVISIÓN DEL CAMINO EN LA RED**

Este comando funciona de forma similar al *ping* solo que de una forma mas detallada nos muestra el camino que sigue una petición al destino final, es decir, nos muestra cuantos saltos (*hops*<sup>61</sup>) hay entre el origen y el destino junto con datos como dirección de *IP* y el tiempo de vida de la

---

<sup>61</sup> Hop: "Término utilizado para denominar cada uno de los pasos que se deben dar para llegar de un punto de origen a otro de destino a lo largo de una Red con la ayuda de routers".

Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar  
conexión (TTL).

```
traceroute google.com  
traceroute 192.168.0.254
```

Hay veces en que la información de un salto no aparece y es reemplazada por asteriscos (\*), esto significa que los nodos están configurados de modo seguro, y esconden esta información como protección ante posibles ataques.

“En conclusión, se puede decir que con este comando se puede detectar cual es la causa de retardo o desconexión en una comunicación con gran detalle<sup>62</sup>”.

---

<sup>62</sup>Cita de Linux, administración del sistema y la red, página 173

## ***APÉNDICES***

**A CLARKCONNECT 4.3**

**B GLOSARIO**

**C BIBLIOGRAFÍA**

## **A CLARKCONNECT 4.3**

Durante la etapa final del desarrollo de este trabajo escrito *Point Clark Networks* liberó la versión 4.3 de la distro *Clarkconnect*, con unos pocos cambios y nuevas funcionalidades. De los nuevos cambios la más útil para un *Firewall* es *System Processes*.

### **A.1 System Processes**

Esta herramienta en *System Settings* permite ver y administrar los procesos que corren en el sistema. La ventana de los procesos nos muestra su nombre, su *PID*, el gasto y consumo de recursos como el procesador y la memoria, adicionalmente podemos conocer quién arrancó el proceso y desde hace cuánto. Con estos datos se pueden determinar procesos potencialmente peligrosos o que puedan comprometer la estabilidad del sistema y de esta forma se obtiene la posibilidad de realizar las siguientes acciones:

[Imagen ape1]

Processes							
	ID	Owner	Running	CPU	Memory	Size	Command
<input type="checkbox"/>	31614	102	00:00:09	1.1 %	3.0 %	6.5 KB	webconfig
<input type="checkbox"/>	31627	102	00:00:09	1.0 %	2.6 %	6.2 KB	webconfig
<input type="checkbox"/>	1630	root	00:00:00	0.3 %	0.4 %	597 Bytes	pluto
<input type="checkbox"/>	18280	root	00:06:47	0.1 %	0.1 %	390 Bytes	pppoe

1. **Detener/Continuar (Pause/Continue) la herramienta:** esta opción detiene la actualización constante de la pantalla para poder estudiar detalladamente los procesos y decidir qué hacer con un determinado proceso.
2. **Mostrar/Ocultar (Show/Hide idle) procesos desocupados:** la mayoría de los procesos en el sistema se encuentran desocupados o durmiendo esperando para poder realizar su tarea cuando sea requerido. Esta opción muestra u oculta de la ventana de procesos los que se encuentran desocupados.
3. **Mostrar/Ocultar (Show/Hide details) detalles de los procesos:** brinda la opción de mostrar u ocultar los detalles de los procesos, los cuales a veces pueden ser poco descriptivos, conocer el nombre del proceso a veces es suficiente.
4. **Matar<sup>63</sup> (Kill) procesos:** con esta opción se “matan” los procesos seleccionados por medio de la casillas que se encuentran delante de cada uno. ¡Atención: esta opción puede afectar la estabilidad del sistema! Para “matar” un proceso se debe seguir este orden:
  - Detener el software que depende del proceso por medio de la herramienta *Running Services*.<sup>64</sup>
  - Detener la actualización de la ventana de procesos.
  - Seleccionar el proceso a “matar” por medio de la casilla
  - Apretar el botón de *Kill* para “matar” el proceso.

<sup>63</sup>Hacer *Kill* a un proceso es enviarle una señal de terminación a éste para poder cerrarlo o terminarlo.

<sup>64</sup>Esta acción evitará posibles problemas con el software y los procesos al momento de detenerlos.

**Nota:** Esta herramienta es similar a *top* o por ende a *htop* por consola, en la sección 6.2 (Monitoreo Remoto de Servidores), puede servir como reemplazo a los programas por consola, de esta manera se puede hacer desde el mismo *Webconfig* el monitoreo al sistema sin necesidad de conectarse remotamente al *Firewall* por *ssh*.

## **B GLOSARIO**

**Adaptador o Tarjeta de Red**, "es el dispositivo que conecta físicamente el ordenador con una red<sup>65</sup>".

**ADSL (Asymmetrical Digital Subscriber Line)**, tecnología similar al DSL para la transmisión de datos digitales a través de líneas telefónicas. Ofrece una conexión permanente a la red.

**Archivo de registro (log file)**, es donde se almacena información de un periodo de tiempo sobre quién, cuando y donde de lo que sucede en un sistema informático como un computador o un servidor. Los administradores pueden luego utilizar estos archivos de texto que comúnmente contienen: fecha, nombre de usuario, actividad y lugar, para examinar las acciones de un usuario o un grupo de usuarios y de ser necesario mostrarlo como evidencia.

**Backup (Copia de seguridad)**, es la copia de los datos originales en un medio digital diferente al que contiene los originales. Se usa para restaurar los datos ante un evento inesperado como una catástrofe o un error del sistema.

**BIOS (Basic Input-Output System)**, sistema básico de entrada-salida. Software básico instalado en la placa base o tarjeta madre que inicia el SO.

**Boot**, término que se refiere a modificar el arranque de los dispositivos de almacenamiento para iniciar con él en primer lugar. O carga de un sistema operativo al iniciarse una máquina.

**Caché**, datos que fueron duplicados de los originales, debido a que los datos originales son costosos de acceder, en tiempo y otros factores, con respecto a la copia existente en el caché. Al acceder por vez primera a

---

65 Cita de: <http://www.mastermagazine.info/termino/3776.php>

un dato, se le hace una copia en el caché, los accesos que siguen al primero se realizan a dicha copia, haciendo que el tiempo de acceso a los datos sea menor.

**Cracker**, persona que por medio de ingeniería inversa realiza: seriales, *keygens*, *cracks* para programas de pago y juegos. También es conocido por violar la seguridad de sistemas informáticos con beneficio propio u lucrativo. Se le nombra así a los “*hackers*” malvados o cuyo fin es hacer mal con sus conocimientos.

**Daemon (Disk And Execution MONitor - Demonio)**, en el mundo *Linux* es un programa o proceso que corre en segundo plano, fuera del control (principal) del usuario.

**DHCP (Dynamic Host Configuration Protocol)**, permite la configuración automática del protocolo *TCP/IP* de todos los clientes en la red. Evita el trabajo de configurar manualmente cada máquina con el protocolo *TCP/IP* cada vez que se agrega a la red, por ejemplo: dirección *IP*, dirección *IP* del servidor *Proxy* o *DNS* y *WINS*. Solo con modificar los parámetros del servidor *DHCP* este cambia los de las terminales de la red automáticamente simplificando el trabajo.

**Dirección IP**, Una dirección numérica por la cual se identifica a un sistema en una red, sea local o en Internet. Consta de cuatro “secciones” divididas por un punto, los números, varían del 0 al 255. Ejemplo: 192.168.1.0 , 200.128.116.22 , 72.14.207.99.

**Dirección MAC (Medium Access Control address)**, identificador de 48 *bits* único para cada tarjeta o interfaz de red. Cada dispositivo que se conecte a una red posee una única dirección. Se le conoce también como dirección física para identificar a dispositivos de red.

**Disco Duro (Hard Disk)**, es uno de los dispositivos mas importantes de un computador, allí se almacena físicamente la información electrónica con la cual trabaja el *software*, por ejemplo: un documento o un programa.

**DNS**, ver Servidor *DNS*.

**Dominio (domain)**, es un nombre (descriptivo) en el cual se agrupan

un sin número de computadores en una red. Los dominios vienen siempre separados por mínimo un punto, el cual diferencia los niveles de los dominios, como dominio de primer nivel (.com, .edu. .gov) y de segundo nivel (cualquienombre, colegioalemanmedellin), y así hasta varios niveles. Un ejemplo de dominio es: colegioalemanmedellin.edu.co. Un dominio es necesario para que las máquinas en la red puedan compartir datos entre si, y este dominio es controlado por un servidor.

**DoS (Ataque de denegación de Servicio, Denial of Service)**, consiste en atacar una red o un sistema, como un servidor, para impedir que un recurso (una página web, un servicio, etc) no este disponible a los usuarios. El alto consumo de ancho de banda que provoca el ataque da la perdida de conectividad sobrecargando al sistema o a la red, logrando finalmente la caída de esta. Este tipo de ataques a redes o sistemas se coordina a través de muchas máquinas las cuales realizan constantemente y por un tiempo prolongado la misma petición de un servicio o recurso.

**DSL (Digital Subscriber Line)**, tecnología para conectarse a internet a través de líneas telefónicas a mayor velocidad. Ofrece una conexión permanente a la red.

**Enlaces de Dispositivos (/dev/sda ; /dev/hda)**, son enlaces que apuntan al hardware de la máquina. En el directorio /dev/ se almacenan estos enlaces, siendo estos todos los dispositivos para los cuales el *Kernel* tiene un *Driver*. Estos enlaces son usados para montar los dispositivos al SO mediante el comando `mount`. Cada dispositivo tiene una nomenclatura asignada, para un disco duro *IDE*, este se identifica como /dev/hda/, si se desea nombrar solo una partición de este, se llama así: /dev/hda1 o /dev/hdb3, siendo el número el indicador de la partición comenzando por 0. Los discos duros *SATA* son /dev/sda y las unidades de *CDROM* son /dev/cdrom.

**EXT3 (third extended filesystem o tercer sistema de archivos extendido)**, es un sistema de archivos, el cual es usado ampliamente por las distribuciones de *Linux*. Este ha evolucionado y mejorado con el tiempo considerándose actualmente un sistema de archivos eficiente.

**Firewall**, es un dispositivo que funciona entre dos o mas redes, permitiendo o denegando las transmisiones de una red a la otra como un policía, 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.

**FTP (File Transfer Protocol)**, se usa para transferir archivos de un sistema a otro. Ejemplo: Se designa una carpeta en un servidor, en la cual se encuentran algunas canciones que deseo que algunas personas puedan descargar o que ellos puedan subir.

**Gateway (Puerta de enlace)**, "dispositivo permite interconectar redes con protocolos y arquitecturas diferentes<sup>66</sup>". Ejemplo: un dispositivo, como un ruteador se conecta a una LAN y al módem de internet, el ruteador permite que los computadores de la LAN puedan salir a internet de una forma sencilla.

**GNU/Linux**, completo sistema operativo libre y gratuito. Es conformado por el proyecto GNU y el núcleo (kernel) Linux. Juntos forman un sistema operativo que es complementado con otras aplicaciones. Ver: <http://www.gnu.org/home.es.html>.

**GRUB (GRand Unified Bootloader)**, gestor de arranque que permite seleccionar un SO para arrancarlo. Se inicia despues del chequeo de la BIOS. Ejemplo: al iniciar la máquina, aparece el GRUB ofreciendo iniciar un determinado SO, si se desea se puede cambiar a otro como Windows; despues de un tiempo determinado el GRUB arranca el SO seleccionado por defecto.

**Hacker**, "es la persona que es capaz de explorar un sistema hasta sus lugares más recónditos, en busca del conocimiento, y en ese camino, consigue el control de los sistemas más complejos. Sea cual sea el sistema, ya que el 'hacking' no está limitado a la tecnología informática: puede haber 'hackers' de la física, de la medicina, del derecho o incluso de la gastronomía." --Entrevista a Carlos Sánchez Almeida, abogado español especializado en Internet, nuevas tecnologías y delitos informáticos.

---

66 Cita de: [http://es.wikipedia.org/wiki/Gateway\\_\(informática\)](http://es.wikipedia.org/wiki/Gateway_(informática))

**Hardware**, componente físico dentro y fuera de un computador. Son los componentes con los cuales el *software* interactúa. Ejemplo: un *mouse*, el teclado, un disco duro.

**Hostname (Nombre de Equipo)**, es el nombre que se le da a una máquina en una red, de esta forma se puede intercambiar información y datos con ella sin tener que conocer la dirección *IP*. Es una forma de identificar a las máquinas en una red.

**HTTPS (Secure Hyper Text Transfer Protocol)**, protocolo de transferencia segura de hipertexto, se usa para realizar conexiones *HTTP* para transferencia de contenido pero de forma segura, empleando algoritmos de cifrado que protegen el contenido.

**IMAP (Internet Message Access Protocol)**, protocolo por el cual se accede a mensajes (correos) electrónicos almacenados en un servidor. Se puede usar cualquier terminal con una conexión a Internet. Este protocolo permite una mejor gestión del correo en el buzón de correo.

**Interfaz de red**, es un medio abstracto por el cual se accede al adaptador de red, se puede configurar y nombrar según sean las necesidades. Esta interfaz es la que se configura, por ejemplo: con una dirección de *IP* para el envío y recibo de paquetes por medio del protocolo *TCP/IP*.

**Interfaz Web (Web Interface)**, interfaz (capa de usuario) de un programa accesible desde un navegador. De esta forma se pueden manejar programas, por ejemplo un servidor, a través de una red.

**Interprete de Ordenes, Consola o Shell**, es un programa, el cual actúa como interfaz de usuario y el SO para comunicarse por medio de ordenes escritas por el usuario. El SO las interpreta y (entrega los resultados) ejecuta la operación indicada. Termina esto, el interprete de ordenes espera por una nueva orden. La interacción entre el individuo y la máquina es únicamente por texto plano. En *Linux* se usa comúnmente el nombre de *Shell*, siendo el mas común el *BASH (Burn Again SHell)*.

**IP**, ver dirección *IP*.

**Jerarquía del Sistema de Archivos en Linux**, es conformado por los

directorios principales con sus contenidos en el SO. Diseñado en 1994 para lograr un estándar en el sistema de archivos de las distribuciones de *GNU/Linux*. Se basa en el diseño en el cual todos los directorios cuelgan de una raíz / sin importar su uso o procedencia (otros sistemas de archivos, como un disco duro externo).

**Kernel o Núcleo (Linux Kernel)**, "se puede definir como el corazón de este sistema operativo<sup>67</sup>". Se encarga que el *software* y el *hardware* de la máquina puedan trabajar juntos, es una capa de conecta a estas dos para lograr un correcto funcionamiento. Sin *Kernel* un SO es solo un montón de software que no se pueden comunicar con el *hardware*. *Linux* es un clon de *UNIX*, fue escrito y diseñado por Linus Torvalds a principios de los noventa. Hoy en día es Software Libre y cuenta con una gran comunidad que apoya su progreso y desarrollo a lo largo del planeta.

**LAN (Local Area Network o red de área local)**, es una red donde dos o más estaciones de trabajo y/o servidores de conectan entre si para compartir datos o simplemente una conexión a Internet u a otra red. Un ejemplo es la red con que se conectan los computadores de una institución u oficina.

**loopback**, "dispositivo de red *loopback* es un interfaz de red virtual<sup>68</sup>" local. Es usado por procesos y programas para comunicarse entre si por medio de protocolos de red. Puede ser usado tambien para conectarse a servicios locales de la máquina.

**Navegador (browser)**, programa que permite visualizar las páginas web presentes en internet por medio del protocolo *HTTP*. Ejemplo: *Internet Explorer* ® o *Mozilla Firefox* ®.

**Nodo (de red)**, es un punto de la red, un sitio donde convergen una o mas conexiones. "Un nodo es un punto de intersección o unión de varios elementos que confluyen en el mismo lugar. En redes cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también un nodo<sup>69</sup>".

**Nombre de Equipo**, ver *Hostname*.

---

67 Cita de: <http://www.linux-es.org/kernel>

68 Cita de: <http://es.wikipedia.org/wiki/Loopback>

69 Cita de: [http://es.wikipedia.org/wiki/Nodo\\_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Nodo_(inform%C3%A1tica))

**MAC**, ver dirección *MAC*.

**Malware**, es un término utilizado para el software malicioso y se refiere a todo *software* creado para realizar acciones no autorizadas o maliciosas. Virus, troyanos, *spyware* y demás son ejemplos de lo que se considera *Malware*.

**Memoria RAM (Random Access Memory)**, es el lugar donde la máquina almacena los datos e información que están siendo utilizados en el momento presente; estos datos permanecen temporalmente allí hasta que la máquina sea apagada o reiniciada. "Se le llama *RAM* por que es posible acceder a cualquier ubicación de ella aleatoria y rápidamente<sup>70</sup>". [Ver adicionalmente: *Swap* o Espacio de Intercambio].

**MIME Type (Multipurpose Internet Mail Extensions)**, es una forma de catalogar a archivos multimedia que no sean textos plano. Es un estándar para diferenciar los diferentes tipos de contenido que se pueden enviar a través del internet o por correo electrónico. En el caso de este trabajo es un tipo de archivo que se puede permitir o denegar para que llegue a la máquina cliente que lo desea recibir o descargar.

**Módulos**, sección de *software* que puede ser fácilmente removida o instalada en un sistema sin afectar la integridad de este. Los módulos de *software* permiten añadir nuevas posibilidad y opciones al Servidor/*Firewall*.

**MySQL**, sistema de gestión de bases de datos de código abierto, muy popular y ampliamente usado por compañías y servidores Web.

**P2P (peer to peer)**, red donde usuarios de Internet (y/o servidores) se conectan entre si a través de programas y protocolos como *Ares* o *eMule* para compartir archivos tales como: música, vídeos, imágenes, programas y documentos. Estas redes *p2p* son conocidas por promover la "piratería" al permitir la descarga de archivos con *Copyright* "ilegalmente"; también por su papel para ayudar a difundir *Malware* a través de Internet. Su ilegalidad es debatible, y las leyes de muchos países, entre ellas la colombiana, establecen que descargar contenido

---

<sup>70</sup>Cita de: <http://www.monografias.com/trabajos11/memoram/memoram.shtml>

con *Copyright* en el computador no es ilegal mientras sea para uso personal y no para algún tipo de lucro u copias indiscriminadas. Por otra parte, compartir este contenido, en otras palabras subirlo a la red, si es ilegal y es penado por la ley.

**POP (Post Office Protocol)**, Protocolo de oficina de correos. Estándar de correo electrónico, usa un buzón para acumular los mensajes de un usuario, hasta que éste se conecta con el servidor para leer ese correo.

**PPPoE (Point-to-Point Protocol over Ethernet o Protocolo Punto a Punto sobre Ethernet)**, es un protocolo de red sobre *Ethernet*. Se utiliza comúnmente para proveer conexión de banda ancha mediante un cable módem. Tiene autenticación y cifrado.

**Procesador, CPU (Central Processing Unit)**, es un chip ("trozo de silicio que contiene millones de componentes electrónicos<sup>71</sup>") el cual interpreta las ordenes y procesa la información que se encuentra en el *software*.

**Protocolo (de red)**, "es un conjunto de reglas establecidas entre dos dispositivos para permitir la comunicación entre ambos<sup>72</sup>". Los protocolos ayudan a evitar la incompatibilidad entre los dispositivos de distintos fabricantes. Existen diferentes protocolos para la comunicación en redes, dos grandes grupos de conocen, Protocolos de Internet como *HTTP* o *FTP* para el intercambio de información como páginas web; por otro lado los Protocolos de Red son los encargados de llevar esta información de un lado a otro, por ejemplo: el Protocolo *TCP/IP*.

**Protocolo HTTP (Hyper Text Transfer Protocol)**, protocolo de transferencia de hipertexto. Se usa como sistema de comunicación y transferencia para visualizar páginas Web desde una navegador como *Internet Explorer*. Este protocolo lo que hace es transferir el contenido: una página Web, un archivo de sonido o una imagen a otro ordenador para que este lo pueda visualizar cuando se pulsa un hiper vínculo.

**Proxy**, permite a varios clientes conectarse a Internet a través de una única conexión física a Internet. Puede permitir, denegar o filtrar el

---

71 Cita de: <http://www.monografias.com/trabajos12/comptcn/comptcn.shtml#UCP>

72 Cita de:

<http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml>

contenido y el uso del Internet en la red. Ejemplo: es como un cuello de botella por donde pasan todas las conexiones.

**Red Hat Linux**, distribución *Linux* de tipo comercial muy popular entre las empresas. Creada y mantenida por la compañía del mismo nombre. Sus programadores han contribuido a la comunidad libre con varias tecnologías y *software*.

**Salto (Hop)**, "Término utilizado para denominar cada uno de los pasos que se deben dar para llegar de un punto de origen a otro de destino a lo largo de una Red con la ayuda de *routers*<sup>73</sup>".

**Samba**, es un software que permite compartir archivos e impresoras con otros computadores en la misma red. Utiliza para ello un protocolo conocido como *SMB/CIFS*.

**Servidor DNS (Domain Name System)**, es un servidor que traduce las peticiones de los clientes en direcciones *IP* para su uso en la red. Ejemplo: `www.google.com --> 72.14.207.99`.

**Servidor**, es un computador o máquina cuyo propósito es proveer datos o servicios de modo que otras máquinas puedan utilizarlos.

**Sistema de Archivos**, es un método para almacenar, organizar y estructurar los archivos e información de una máquina, facilitando el acceso a los datos. Los sistemas de archivos usan una unidad de almacenamiento, comúnmente un disco duro, para guardar y organizar estructuralmente la información.

**Sistema operativo**, es el programa (o *software*) más importante de un computador destinado a permitir una gestión eficaz de sus recursos. Comienza a trabajar cuando se enciende el computador, y gestiona el *hardware* de la máquina desde los niveles más básicos, permitiendo también la interacción con el usuario.

**SMTP (Simple Mail Transfer Protocol)**, protocolo de transferencia simple de correo, por el cual se envía (exclusivamente) correo

---

<sup>73</sup>Cita de:

[http://www.embusca.gob.mx/wb2/eMex/eMex\\_Glosario\\_de\\_terminos\\_Seguridad?page=28](http://www.embusca.gob.mx/wb2/eMex/eMex_Glosario_de_terminos_Seguridad?page=28)

electrónico en Internet.

**Software**, conjunto de ordenes que forman un programa que se ejecuta en el *hardware*. Son los programas de un computador como el SO, un navegador o el *kernel* de *Linux*.

**SPAM**, mensajes de correo electrónico no solicitados, habitualmente de tipo publicitario, enviados en forma masiva.

**Superusuario o root**, es aquel que administra los sistemas *Unix* o *Linux*. Este es responsable de administrar y configurar el sistema, es el único con permisos para añadir o remover usuarios, para instalar *software*, configurar nuevos dispositivos, etc. No se recomienda trabajar normalmente como superusuario ya que cualquier error siendo este usuario puede comprometer enteramente el SO, solo usar lo estrictamente necesario.

**Swap o Espacio de Intercambio**, es el espacio del disco duro asignado para ser usado como una "ampliación" de la Memoria *RAM* y poder así guardar los datos que excedan el espacio de la misma. Se usa también como caché de la *RAM* para mantenerla libre de los programas que no están en uso y logrando proveer mas espacio a los procesos y programas que si necesitan una memoria mas rápida.

**TCP (Transmission Control Protocol)**, usado para realizar conexiones fiables a través de la red entre dos programas. Garantiza que la comunicación se buena y que los paquetes si lleguen a su destino. Ver *UDP*.

**TCP/IP**, protocolo para la comunicación fiable de datos en una de red, es uno de los protocolos mas ampliamente usados en el mundo. Creado por la *DARPA* y usado por primera vez en 1972 en la *ARPANET*. El nombre del protocolo proviene de la unión de dos protocolos importantes "el *Transmission Control Protocol (TCP)* y el *Internet Protocol (IP)*. Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto<sup>74</sup>". El *TCP/IP* es la base bajo la cual el Internet esta construido.

---

74Cita de:

<http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml>

**TTL (Time To Live)**, es parte de la estructura de un paquete de red, el cual indica el máximo de nodos o ruteadores por lo que puede pasar antes de ser descartado o devuelto a su origen.

**UDP (User Datagram Protocol)**, se usa para enviar mensajes a través de la red sin garantía que exista una respuesta o que el paquete haya alcanzado a su destino. Ver *TCP*.

**Unidades de CD-ROM, DVD-ROM**, son unidades para el almacenamiento de datos e información físicamente, estos dispositivos son normalmente externos y se pueden transportar fácilmente. Si espacio a aumentado gradualmente con el venir de los años.

**UNIX**, Sistema operativo multiusuario basado en un kernel, desarrollado por los laboratorios *Bell* de *AT&T* en 1969. Estable, "portable" y seguro. El *kernel Linux* y el entorno *GNU* están basados en este SO. Y son sus variantes mas famosas actualmente. Caracterizado por: ser multiusuario, escrito en lenguaje de alto nivel C, programable por medio de una consola de comandos, maneja la memoria dinámicamente, permite la comunicación entre procesos, "emplea un sistema jerárquico de archivos, con facilidades de protección de archivos, cuentas y procesos". Visitar: <http://www.gnu.org/home.es.html>.

**UPS (Uninterruptible Power Supply)**, sistema de alimentación ininterrumpida, es un dispositivo, el cual por medio de baterías puede alimentar a otros dispositivos con energía eléctrica por un tiempo limitado. Se usan para garantizar el flujo constante de energía eléctrica para servidores y máquinas, mientras se controla y se mejora la calidad de esta.

**URL (Uniform Resource Locator)**, Localizador Unificado de Recursos. Dirección a través de la cual se accede a las páginas Web en Internet o a otros ordenadores en la red. Ejemplo: [www.google.com](http://www.google.com), \\PC1.

**VPN (Virtual Private Network)**, Red Privada Virtual. Conexión entre dos o mas sistemas a través de una red publica como Internet para intercambiar información de forma segura y cifrada.

**WINS**, es la aplicación de *Microsoft* que resuelve los nombres *NetBIOS*,

los cuales son usados para referirse a otra máquina en una red sin tener que conocer su dirección de *IP*. Ejemplo: si deseamos conectarnos al servidor de archivos podemos teclear en un navegador: `http://servarchivos.lan` en ves de teclear su dirección de *IP*: 192.168.1.83. *WINS* lo que hace es cambiar los nombres por direcciones *IP*, siendo este proceso transparente para el usuario.

## **C BIBLIOGRAFÍA**

"Sistema Operativo" [en línea]. Autores: Danny Gonzales y Eduard Alaniz, alojado en Monografias.com.  
[http://www.monografias.com/Computacion/Sistemas\\_Operativos](http://www.monografias.com/Computacion/Sistemas_Operativos)  
[Consulta: 12 enero 2008]

"¿Qué es un Sistema Operativo?" [en línea]. FAQ de masadelante.com.  
<http://www.masadelante.com/faq-sistema-operativo.htm>  
[Consulta: 12 enero 2008]

"¿Qué es el proyecto GNU?" [en línea]. Autor: La comunidad GNU.  
<http://www.gnu.org/home.es.html>  
[Consulta: 12 ene. 2008]

"¿Qué es un servidor? - Definición de servidor" [en línea]. FAQ de masadelante.com.  
<http://www.masadelante.com/faq-servidor.htm>  
[Consulta: 12 enero 2008]

"Beneficios de un Firewall en Internet" [en línea]. Autor: Víctor Ferrusola.  
[http://lanrouter.com/index.php?option=com\\_content&task=view&id=38&Itemid=71](http://lanrouter.com/index.php?option=com_content&task=view&id=38&Itemid=71)  
[Consulta: 12 enero 2008]

"Sistema operativo UNIX" [en línea]. Trabajo realizado por: Martinoli Diego, alojado en Monografias.com.  
<http://www.monografias.com/trabajos/UNIX/UNIX.shtml>  
[Consulta: 16 enero 2008]

"Malware" [en línea]. Sección amenazas en:  
<http://usa.kaspersky.com/threats/Malware.php>  
[Consulta: 16 enero 2008].

"SPAM" [en línea]. Por Cristian Borghello.

<http://www.segu-info.com.ar/Malware/SPAM.htm>

[Consulta: 16 enero 2008]

"Normas sobre el funcionamiento de los establecimientos que prestan el servicio de Internet en Bogotá, D.C" [en línea]. Publicado por 4v4t4r en 'Legislación y ética'. Febrero 11 de 2008.

<http://www.dragonjar.org/normas-sobre-el-funcionamiento-de-los-establecimientos-que-prestan-el-servicio-de-Internet-en-bogota-dc.xhtml>

[Consulta: 14 de febrero de 2008]

"Glosario de seguridad informática" [en línea]. Publicado por 4v4t4r en 'Conceptos / Definiciones'. 19 de julio de 2007.

<http://www.dragonjar.org/glosario-de-seguridad-informatica.xhtml>

[Consulta: 25 de marzo de 2008]

"Glosario de seguridad informática parte 2" [en línea]. Publicado por 4v4t4r en 'Conceptos / Definiciones'. 19 de julio de 2007.

<http://www.dragonjar.org/glosario-de-seguridad-informatica-parte-2.xhtml>

[Consulta: 25 de marzo de 2008]

"Terms of Service" [en línea]. Point Clark Networks. Toronto, Canada.

[http://www.clarkconnect.com/about/tos\\_pcn.php](http://www.clarkconnect.com/about/tos_pcn.php)

[Consulta: 20 de marzo de 2008]

"PPPoE" [en línea]. Anónimo. Bajo licencia GNU.

<http://es.wikipedia.org/wiki/PPPoE>

[Consulta: 20 de marzo de 2008]

"User Guide" [en línea]. Point Clark Networks. Toronto, Canada.

<http://www.clarkconnect.com/help/userguide/>

[Consulta: 20 de marzo de 2008]

“Linux - Estructura de árbol de archivos, Jerarquía de archivos en Linux” [en línea]. Autor: es.kioskea.net, texto bajo la licencia Creative Commons.

<http://es.kioskea.net/linux/linarb.php3>

[Consulta: 20 de marzo de 2008]

“Red Hat Linux” [en línea]. Anónimo. Bajo licencia GNU. En wikipedia.org.

[http://es.wikipedia.org/wiki/Red\\_Hat\\_Linux](http://es.wikipedia.org/wiki/Red_Hat_Linux)

[Consulta: 24 de marzo de 2008]

“Que es bootear????” [en línea]. Usuarios de Yahoo Answers. En answers.yahoo.com.

<http://es.answers.yahoo.com/question/index?>

[qid=20061003235007AACbF1F](http://es.answers.yahoo.com/question/index?qid=20061003235007AACbF1F)

[Consulta: 24 de marzo de 2008]

“Arranque” [en línea]. Anónimo. Bajo licencia GNU. En wikipedia.org.

<http://es.wikipedia.org/wiki/Arranque>

[Consulta: 24 de marzo de 2008]

“BIOS” [en línea]. Anónimo. Bajo licencia GNU. En wikipedia.org.

<http://es.wikipedia.org/wiki/BIOS>

[Consulta: 24 de marzo de 2008]

“¿Qué es... la BIOS?” [en línea]. Juan Herrerías Rey. En conozcasuhardware.com.

<http://www.conozcasuhardware.com/quees/bios1.htm>

[Consulta: 24 de marzo de 2008]

“El superusuario” [en línea]. Felipe Gabaldon Castillo. 2005-05-20. En w3.mecanica.upm.es.

[http://w3.mecanica.upm.es/~felipe/meKNOPPIX/survival\\_html/nod](http://w3.mecanica.upm.es/~felipe/meKNOPPIX/survival_html/nod)  
[e7.html](http://w3.mecanica.upm.es/~felipe/meKNOPPIX/survival_html/nod)

[Consulta: 24 de marzo de 2008]

“Qué es DHCP” [en línea]. Pedro Pablo Fábrega. En dns.bdat.net.

<http://dns.bdat.net/dhcp/c33.html#AEN36>

[Consulta: 25 de marzo de 2008]

“Selección de soluciones Hardware y Software” [en línea]. Por Evolucy Technology Consulting S.L. En [evolucy.com](http://evolucy.com).  
[http://www.evolucy.com/esp/software\\_abierto/seleccion\\_hardware\\_software.php](http://www.evolucy.com/esp/software_abierto/seleccion_hardware_software.php)  
[Consulta: 30 de marzo de 2008]

“Arrancar desde el CD” [en línea]. Contenido con licencia Creative Commons. En [guia-ubuntu.org/](http://guia-ubuntu.org/)  
[http://www.guia-ubuntu.org/index.php?title=Arrancar\\_desde\\_el\\_CD](http://www.guia-ubuntu.org/index.php?title=Arrancar_desde_el_CD)  
[Consulta: 1 de abril de 2008]

“ADMINISTRACIÓN DE UN CENTRO DE CÓMPUTO” [en línea]. Por [personales.com](http://personales.com).  
<http://personales.com/mexico/culiacan/administracion/>  
[Consulta: 1 de abril de 2008]

“Web Interface” [en línea]. Por Telekom. En [kmu.telekom.at](http://kmu.telekom.at).  
<http://kmu.telekom.at/glossar/suche/suche.php?buchstabe=W>  
[Consulta: 14 de abril de 2008]

“Línea de comandos” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://wikipedia.org).  
[http://es.wikipedia.org/wiki/L%C3%ADnea\\_de\\_comandos](http://es.wikipedia.org/wiki/L%C3%ADnea_de_comandos)  
[Consulta: 9 de junio de 2008]

“¿Qué es WINS?” [en línea]. Prof. Luis M. Cardona Hernández. En [bc.inter.edu](http://bc.inter.edu).  
<http://bc.inter.edu/facultad/LCARDONA/InfGen/WINS&DNS.htm>  
[Consulta: 10 de junio de 2008]

“Caché” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://wikipedia.org).  
<http://es.wikipedia.org/wiki/Cach%C3%A9>  
[Consulta: 11 de junio de 2008]

“Load (computing)” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://wikipedia.org).  
[http://en.wikipedia.org/wiki/Load\\_\(computing\)](http://en.wikipedia.org/wiki/Load_(computing))  
[Consulta: 24 de junio de 2008]

“Snort” [en línea]. Escuela Universitaria de Ingeniería Técnica en Informática de Oviedo. En [euitio178.ccu.uniovi.es](http://euitio178.ccu.uniovi.es).  
<http://euitio178.ccu.uniovi.es/wiki/index.php/Snort>  
[Consulta: 26 de junio de 2008]

“Format” [en línea]. Steven Sturges 2008-05-28. En [snort.org](http://www.snort.org).  
[http://www.snort.org/docs/snort\\_htmanuals/htmanual\\_282/node220.html#example\\_classification\\_rules](http://www.snort.org/docs/snort_htmanuals/htmanual_282/node220.html#example_classification_rules)  
[Consulta: 26 de junio de 2008]

“Tar” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://es.wikipedia.org).  
<http://es.wikipedia.org/wiki/Tar>  
[Consulta: 29 de junio de 2008]

“Understanding the Routing Table” [en línea]. Por Ktec Training. En [ktectraining.com](http://www.ktectraining.com).  
[http://www.ktectraining.com/demo/Demo3/Network%20Infrastructure%2070-291%20Part%204/page\\_05.html](http://www.ktectraining.com/demo/Demo3/Network%20Infrastructure%2070-291%20Part%204/page_05.html)  
[Consulta: 2 de julio de 2008]

“System Monitoring” [en línea]. Por Lars Wirzenius , Joanna Oja , Stephen Stafford, Alex Weeks. En [tldp.org](http://tldp.org).  
<http://tldp.org/LDP/sag/html/system-monitoring.html>  
[Consulta: 15 de julio de 2008]

“Kudzu” [en línea]. Por Red Hat. En [rhlinux.redhat.com](http://rhlinux.redhat.com).  
<http://rhlinux.redhat.com/kudzu/>  
[Consulta: 23 de julio de 2008]

“Sistemas de ficheros” [en línea]. Por ibiblio, the public's library and digital archive. En [ibiblio.org](http://www.ibiblio.org).  
<http://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCaS/doc-unixsec/unixsec-html/node54.html>  
[Consulta: 27 de julio de 2008]

“File system” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://en.wikipedia.org).  
[http://en.wikipedia.org/wiki/File\\_system](http://en.wikipedia.org/wiki/File_system)  
[Consulta: 5 de agosto de 2008]

“Espacio swap/de intercambio” [en línea]. Por Whiskola el 06-10-2005.

En [preguntaslinux.org](http://preguntaslinux.org).

<http://preguntaslinux.org/-guia-espacio-swap-de-intercambio-t-57.html>

[Consulta: 5 de agosto de 2008]

“Que es el kernel/núcleo?” [en línea]. Por Rafael Martinez. Contenido con licencia Creative Commons. En [linux-es.org](http://linux-es.org).

<http://www.linux-es.org/kernel>

[Consulta: 5 de agosto de 2008]

“Protocolos de Red: Protocolo TCP/IP” [en línea]. Por Julio César Chavez Urrea. En [monografias.com](http://monografias.com).

<http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml>

[Consulta: 5 de agosto de 2008]

“El computador - ¿ Que es UCP o CPU ?” [en línea]. Por Yucelis Montilla, Roberth Atencio, Andris Ruiz, Ender Campos. En [monografias.com](http://monografias.com).

<http://www.monografias.com/trabajos12/comptcn/comptcn.shtml#UCP>

[Consulta: 5 de agosto de 2008]

“Memorias RAM” [en línea]. Por Gabriel Echeverria, Claudio Moran M. En [monografias.com](http://monografias.com).

<http://www.monografias.com/trabajos11/memoram/memoram.shtml>

[Consulta: 5 de agosto de 2008]

“¿Qué es un Disco Duro? - Definición de Disco Duro” [en línea]. En [masadelante.com](http://masadelante.com).

<http://www.masadelante.com/faq-disco-duro.htm>

[Consulta: 6 de agosto de 2008]

“Definición de Adaptador de Red” [en línea]. Por MasterMagazine. En [mastermagazine.info](http://mastermagazine.info).

<http://www.mastermagazine.info/termino/3776.php>

[Consulta: 6 de agosto de 2008]

“Interfaces de red” [en línea]. Por Olaf Kirch, Terry Dawson. En [es.tldp.org](http://es.tldp.org).  
<http://es.tldp.org/Manuales-LuCAS/GARL2/gar12/x-087-2-issues.interfaces.html>  
[Consulta: 6 de agosto de 2008]

“Dominio (redes informáticas)” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://es.wikipedia.org).  
[http://es.wikipedia.org/wiki/Dominio\\_\(redes\\_informáticas\)](http://es.wikipedia.org/wiki/Dominio_(redes_informáticas))  
[Consulta: 6 de agosto de 2008]

“Ataque de denegación de servicio” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://es.wikipedia.org).  
[http://es.wikipedia.org/wiki/Ataque\\_de\\_denegación\\_de\\_servicio](http://es.wikipedia.org/wiki/Ataque_de_denegación_de_servicio)  
[Consulta: 6 de agosto de 2008]

“Qué son los MIME Types” [en línea]. Por Duamu.com.  
<http://www.duamu.com/re/articulo/1346/id/549/articulos-que-son-los-mime-types.html>  
[Consulta: 6 de agosto de 2008]

“SALTO (Hop)” [en línea]. Por Portal seguridad en Internet / Sistema Nacional e-México. En [embusca.gob.mx](http://www.embusca.gob.mx).  
[http://www.embusca.gob.mx/wb2/eMex/eMex\\_Glosario\\_de\\_terminos\\_Seguridad?page=28](http://www.embusca.gob.mx/wb2/eMex/eMex_Glosario_de_terminos_Seguridad?page=28)  
[Consulta: 9 de agosto de 2008]

“Nodo (informática)” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://es.wikipedia.org).  
[http://es.wikipedia.org/wiki/Nodo\\_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Nodo_(inform%C3%A1tica))  
[Consulta: 10 de agosto de 2008]

“Sistema de alimentación ininterrumpida” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://es.wikipedia.org).  
[http://es.wikipedia.org/wiki/Sistema\\_de\\_alimentaci%C3%B3n\\_ininterrumpida](http://es.wikipedia.org/wiki/Sistema_de_alimentaci%C3%B3n_ininterrumpida)  
[Consulta: 19 de agosto de 2008]

“Particionar el disco duro” [en línea]. Por Oscar Fernandez López. En [fernandlopez.com](http://www.fernandlopez.com).  
<http://www.fernandlopez.com/linuxfacil/aclaraciones/particiones.htm>  
[Consulta: 23 de agosto de 2008]

“Definición de Hardware” [en línea]. Por ALEGSA. En [alegsa.com.ar](http://www.alegsa.com.ar).  
<http://www.alegsa.com.ar/Dic/hardware.php>  
[Consulta: 31 de agosto de 2008]

“GNU GRUB” [en línea]. Por Yoshinori K. Okuji . En [gnu.org](http://www.gnu.org).  
<http://www.gnu.org/software/grub/>  
[Consulta: 31 de agosto de 2008]

“Definición de DSL” [en línea]. Por ALEGSA. En [alegsa.com.ar](http://www.alegsa.com.ar).  
<http://www.alegsa.com.ar/Dic/dsl.php>  
[Consulta: 4 de septiembre de 2008]

“Definición de ADSL” [en línea]. Por ALEGSA. En [alegsa.com.ar](http://www.alegsa.com.ar).  
<http://www.alegsa.com.ar/Dic/adsl.php>  
[Consulta: 4 de septiembre de 2008]

“Gateway (informática)” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://es.wikipedia.org).  
[http://es.wikipedia.org/wiki/Gateway\\_\(informática\)](http://es.wikipedia.org/wiki/Gateway_(informática))  
[Consulta: 4 de septiembre de 2008]

“Daemon\_(computer\_software)” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://en.wikipedia.org).  
[http://en.wikipedia.org/wiki/Daemon\\_\(computer\\_software\)](http://en.wikipedia.org/wiki/Daemon_(computer_software))  
[Consulta: 4 de septiembre de 2008]

“Loopback” [en línea]. Anónimo. Bajo licencia GNU. En [wikipedia.org](http://es.wikipedia.org).  
<http://es.wikipedia.org/wiki/Loopback>  
[Consulta: 4 de septiembre de 2008]

“Linux, Administracion del sistema y la red”. Por Iñaki Alegría Loinaz, Roberto Cortiñas Rodríguez y Aitzol Ezeiza Ramos. Año 2005. Editorial Pearson, Prentice Hall (Pearson Educación), Madrid. ISBN: 84-205-4848-0.

Entrevista con Carlos Sánchez Almeida, abogado español especializado en Internet, nuevas tecnologías y delitos informáticos.  
Realizada por Pablo Romero para: [elmundo.es](http://elmundo.es). España, 14 de enero de 2008. <http://www.bufetalmeida.com/?id=227>  
[Consulta: 16 de enero 2008]

Imagen >82< obtenida de:  
<http://www.clarkconnect.com/wiki/images/7/77/Squid1.png>  
[Consulta: 10 de octubre 2008]

Imagen >83< obtenida de:  
<http://www.clarkconnect.com/wiki/images/a/a8/Squid2.png>  
[Consulta: 10 de octubre 2008]

Imagen >ape1< obtenida de:  
[http://www.clarkconnect.com/wiki/images/5/5e/Ss\\_processes.png](http://www.clarkconnect.com/wiki/images/5/5e/Ss_processes.png)  
[Consulta: 10 de octubre 2008]

Las capturas de pantalla (screenshots) aquí empleadas fueron tomadas con emuladores de máquinas virtuales QEMU y VMWare Server.  
[www.vmware.com/](http://www.vmware.com/)  
<http://bellard.org/qemu/>

Los nombres Internet Explorer y Windows son propiedad de Microsoft.  
El nombre ClarkConnect y el logo son propiedades de Point Clark Networks.