DISEÑO E IMPLEMENTACIÓN
SERVIDORES/FIREWALL GNU-LINUX CON CONEXIÓN WAN

JUAN CAMILO MIRANDA JIMÉNEZ
WILMER JOSÉ PADILLA GUZMÁN

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS
2010

DISEÑO E IMPLEMENTACIÓN SERVIDORES/FIREWALL GNU-LINUX CON CONEXIÓN WAN

JUAN CAMILO MIRANDA JIMÉNEZ
WILMER JOSÉ PADILLA GUZMÁN

Monografía presentada para optar el título de Ingeniero de Sistemas.

Director
GONZALO GARZÓN
Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS
2010

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias, Diciembre de 2010

Señores:

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
Comité de Evaluación de Proyectos
Escuela de Ingenierías
La Ciudad

Respetados Señores:
Cordial saludo, nos dirigimos a ustedes con el fin de presentar para su estudio, consideración y aprobación la monografía titulada "*DISEÑO E IMPLEMENTACIÓN SERVIDOR/FIREWALL GNU-LINUX CON CONEXION WAN*", cómo requisito parcial para optar el título de Ingeniero de Sistemas.

Atentamente,

Juan Camilo Miranda Jiménez

Wilmer José Padilla Guzmán

Cartagena de Indias, Diciembre de 2010

Señores:

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
Comité de Evaluación de Proyectos
Escuela de Ingenierías
La Ciudad

Respetados Señores:
Cordial saludo, nos dirigimos a ustedes con el fin de presentar para su estudio, consideración y aprobación la monografía titulada "*DISEÑO E IMPLEMENTACIÓN SERVIDOR/FIREWALL GNU-LINUX CON CONEXION WAN*", para su estudio y evaluación, la cual fue realizada por los estudiantes JUAN CAMILO MIRANDA JIMÉNEZ y WILMER JOSÉ PADILLA GUZMÁN del cual acepto ser su director.

Cordialmente,

_____

Gonzalo Garzón
Ingeniero de sistemas

AUTORIZACIÓN

Cartagena D.T.H. y C. Diciembre de 2010

Yo JUAN CAMILO MIRANDA JIMÉNEZ, identificado con número de cedula 1’047.389.054 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso y publicación de mi trabajo de grado en el catalogo on-line de la Biblioteca.

Juan Camilo Miranda Jiménez
C.C. 1’047.389.054 Cartagena

AUTORIZACIÓN

Cartagena D.T.H. y C. Diciembre de 2010

Yo WILMER JOSÉ PADILLA GUZMÁN, identificado con número de cedula 73’208.165 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso y publicación de mi trabajo de grado en el catalogo on-line de la Biblioteca.

Wilmer José Padilla Guzmán
C.C. 73’208.165 Cartagena

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLA

INTRODUCCIÓN

Hacking ha existido poco más o menos desde el desarrollo de los primeros ordenadores electrónicos. El significado moderno del término hacker[1] tiene sus orígenes en los años 60 y en el Club de Modelaje de Trenes del Instituto de Tecnología de Massachusetts (MIT), que diseñaban conjuntos de trenes de gran escala y detalle.

Desde ese momento el término hacker se ha utilizado para describir cualquier cosa desde un aficionado a las computadoras hasta un programador virtuoso. Un rasgo característico de un hacker es su disposición de explorar en detalle cómo funcionan los sistemas de computación. La prensa usualmente utiliza este término para describir aquellos que accedan sistemas y redes ilegalmente sin escrúpulos, con intenciones maliciosas o criminales. El término más adecuado para este tipo de hacker de computadoras es cracker o maleante informático (también se les conoce como pirata informático, ciberpirata, etc.)— un término creado por los hackers en la mitad de los 80 para diferenciar a las dos comunidades.

En la actualidad, nos encontramos en una evolución continua en las tecnologías de comunicación y transferencia de información que conllevan a una interacción de redes y un mayor volumen de envió de paquetes de datos de forma permanente lo que implica a mayores riesgos a la seguridad de la información de una organización.

El objetivo fundamental de esta monografía es brindar una solución a una red telemática que este expuesta a la inseguridad que hoy nos brinda el internet, gracias a los hackers que están día a día investigando y tratando de buscar la forma de ingresar de forma ilegal a sistemas informáticos que no cuenten con una buenas herramientas de seguridad, es por esto que la seguridad informática se ha vuelo un tema de gran interés para las pymes[2] y grandes empresas del mundo.

Se busca por medio de este documento una solución a esta problemática con la implementación de un servidor/firewall GNU-Linux[3] el cual permita gozar una buena seguridad a los usuarios de una red telemática. Este documento explicara a detalle el paso a paso de la de la implementación de un servidor/firewall GNU-Linux desde sus requerimientos para instalación, configuración y aplicación de normativas o reglas con las cuales vamos a tener una red más segura.

---

[1] http://www.lawebdelprogramador.com/diccionario/#
[2] PYMES: sigla que significa equeñas y medianas empresas
[3] http://www.hispalinux.es/GNULinux

Se espera que con esta monografía y con la implementación de un servidor/firewall GNU-Linux la comunidad informática logre un mayor control del contenido que los usuarios visitan y comparten en Internet en las diferentes redes telemáticas, teniendo un mejor control de la misma.

Escogiendo un computador con el hardware necesario para la instalación de un Servidor/Firewall GNU/Linux, se documenta todo este proceso. 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.

Se otorgará a la comunidad informática el proceso de implementación de un firewall para garantizar la seguridad en una red local y/o Internet.

Conocerá las características principales de los Firewalls, tales como su concepto, ventajas y desventajas, tipos de firewalls y las arquitecturas más utilizada en la actualidad.

Con este documento se dará a conocer cómo funciona la herramienta *ClarkConnect Community Edition 5.0*[4] *o Firestarter*[5] como *Servidor/Firewall GNU-Linux*, además, como son las reglas según las políticas de seguridad.

Se realizarán pruebas que comprueben el éxito de cada una de las topologías y también se filtrará el contenido al cual los usuarios acceden.

A continuación, en el capítulo 1, se encontrará un preámbulo para realizar la implementación de un servidor firewall; en los capítulos 2, se observarán las herramientas utilizadas para el diseño e implementación del firewall; y en el capítulo 3, la implementación de las prácticas realizadas en esta monografía.

[4] http://www.ClarkConnect.com/legacy/index.php
[5] http://www.fs-security.com/docs.php

1. GENERALIDADES DE LA IMPLEMENTACIÓN DE FIREWALL

Al momento de realizar la implementación de un firewall es necesario conocer algunos conceptos relacionados con este dispositivo o programa que protege de ataques o accesos no permitidos a un sistema o red en general.

1.1. HACKER

Es aquella persona que viola un código y obtiene un ingreso ilegal a un sistema computarizado (ya sea una PC personal o una red bancaria), explorando en los sistemas para probar su vulnerabilidad, cometer un delito u obtener cierto beneficio. En la actualidad, existen varios tipos de hackers, entre los que se incluyen los llamados "crackers[6]".[7]

1.1.1. PASOS PARA HACKEAR[8]

1. Introducirse en el sistema que tengamos como objetivo.
2. Una vez conseguido el acceso, obtener privilegios de root (superusuario).
3. Borrar las huellas.
4. Poner un Sniffer[9] para conseguir logins de otras personas.

1.2. ATAQUES A NUESTRA INFORMACIÓN, ¿CUÁLES SON LAS AMENAZAS?[10]

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde donde), es tan importante como saber con qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo.

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

---

[6] un hacker con intenciones destructivas o delictivas.
[7] http://www.alegsa.com.ar/Dic/hacker.php
[8] http://hackearelbruto.blogspot.es/
[9] programa de captura de las tramas de red.
[10] http://www.monografias.com/trabajos16/seguridad-informatica/seguridad-informatica.shtml#ataques

Genios informáticos, por lo general veinteañeros, se lanzan desafíos para quebrar tal o cual programa de seguridad, captar las claves de acceso a computadoras remotas y utilizar sus cuentas para viajar por el Ciberespacio, ingresar a redes de datos, sistemas de reservas aéreas, bancos, o cualquier otra "cueva" más o menos peligrosa.

Los administradores de todos los sistemas, disponen de herramientas para controlar que "todo vaya bien", si los procesos son los normales o si hay movimientos sospechosos, por ejemplo que un usuario esté recurriendo a vías de acceso para las cuales no está autorizado o que alguien intente ingresar repetidas veces con claves erróneas que esté probando.

1.3. HISTORIA DEL FIREWALL

La tecnología de firewall surgió en la década de 1980, cuando Internet era una tecnología bastante nueva en términos de su uso y conectividad mundial. Los predecesores de los cortafuegos de seguridad de la red fueron los routers utilizados en la década de 1980 a las redes separadas unas de otras. La visión de Internet como una comunidad relativamente pequeña de los usuarios de compatibles, que valoraban la apertura para el intercambio y la colaboración había terminado por un número de las principales brechas de seguridad de Internet que se produjo en la década de 1980:

- Clifford Stoll 's descubrimiento de espías alemanes manipulación de su sistema.
- Bill Cheswick "Evening con Berferd" de 1992, en el que se instaló una cárcel electrónica simple para observar a un atacante.
- En 1988, un empleado de la NASA Ames Research Center en California, envió una nota por correo electrónico a sus colegas que decía: "Actualmente, estamos bajo ataque de un virus de Internet, ha llegado a Berkeley, UC San Diego, Lawrence Livermore, de Stanford, y Ames NASA. "
- El Gusano Morris propagación a través de múltiples vulnerabilidades en las máquinas de la época. Aunque no fue maliciosa en su intención, el gusano de Morris fue el primer ataque a gran escala sobre la seguridad en Internet, a la comunidad en línea no era ni esperando un ataque, ni preparada para hacer frente a uno.

Primera generación - los filtros de paquetes[11]

El primer artículo publicado en la tecnología de servidor de seguridad fue en 1988, cuando los ingenieros de Digital Equipment Corporation (DEC) desarrollado sistemas de filtrado

[11] http://www.worldlingo.com/ma/enwiki/es/Firewall

conocido como los cortafuegos de filtrado de paquetes. Este sistema bastante básico era la primera generación de lo que se convirtió en una técnica altamente desarrollada y característica de seguridad de Internet. Los filtros de paquetes acto mediante la inspección de los "paquetes" que representan la unidad básica de transferencia de datos entre computadoras en Internet. Si un paquete coincide con el filtro de paquetes de conjunto de reglas, el filtro de paquetes se reducirá (descartar silenciosamente) el paquete, o rechazarlo (desprenderse de ellos, y enviar a "las respuestas de error" a la fuente).

Segunda generación - la capa de aplicación[12]

El beneficio clave de la capa de aplicación de filtrado es que puede "comprender" determinadas aplicaciones y protocolos (como el File Transfer Protocol, DNS, o navegación por Internet), y se puede detectar si un protocolo no deseados se coló a través de un puerto no estándar o si un protocolo está siendo abusado de alguna manera perjudicial.

Tercera generación - "stateful" filtros[13]

De 1989-1990 a tres colegas de AT & T Bell Laboratories, Dave Presetto, Janardan Sharma, y Kshitij Nigam desarrollado la tercera generación de servidores de seguridad, llamándolos cortafuegos a nivel de circuito. Esta tecnología se conoce generalmente como una inspección de estado de paquetes, ya que mantiene un registro de todas las conexiones que pasa por el cortafuego. Este tipo de servidor de seguridad puede ayudar a prevenir ataques que se aprovechan de las conexiones existentes o las negaciones algunas de los ataques al servicio.

La evolución posterior[14]

En 1992, Bob Braden y Annette DeSchon en la Universidad de Southern California (USC) se refiere el concepto de un firewall. El producto conocido como "Visas", fue el primer sistema que tiene una interfaz de integración visual con colores e iconos, que puedan aplicarse fácilmente y acceder a un sistema operativo, como Microsoft 's Windows o MacOS de Apple. En 1994, una compañía israelí llamada Check Point Software Technologies lo construyó y es conocido como FireWall-1.

[12] http://www.worldlingo.com/ma/enwiki/es/Firewall
[13] http://www.worldlingo.com/ma/enwiki/es/Firewall
[14] http://www.worldlingo.com/ma/enwiki/es/Firewall

1.4. FIREWALL

Es un dispositivo o programa orientado a proteger de ataques o accesos no permitidos a un sistema o red en general. Esto se logra mediante una definición de reglas de acceso.[15]

1.4.1. LOS COMPONENTES DEL SISTEMA FIREWALL[16]

Un Firewall típico se compone de uno, o una combinación, de:

- Ruteador Filtra-paquetes.
- Gateway a nivel-aplicación.
- Gateway a nivel-circuito.

Ruteador Filtra-paquetes: el ruteado toma las decisiones de rehusar y permitir el paso de cada uno de los paquetes que son recibidos. Este sistema se basa en el examen de cada datagrama enviado y cuenta con una regla de revisión de información de los encabezados IP, si estos no corresponden a las reglas, se descarta o desplaza el paquete.

Gateway a nivel-aplicación: los Gateway nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes.

Gateway a nivel-circuito: un Gateway a nivel-circuito es en sí una función que puede ser perfeccionada en un Gateway a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

1.4.2. CARACTERÍSTICAS Y VENTAJAS DEL FIREWALL[17]

- *Protección de la Red*: mantiene alejados a los piratas informático (crackers) de su red al mismo tiempo que permite acceder a todo el personal de la oficina.
- *Control de acceso a los recursos de la red*: al encargarse de filtrar, en primer nivel antes que lleguen los paquetes al resto de las computadoras de la red, el firewall es idóneo para implementar en el los controles de acceso.
- *Control de uso de Internet*: permite bloquear el material no- adecuado, determinar que sitios que puede visitar el usuario de la red interna y llevar un registro.

[15] http://www.seguridadinformatica.dcyc.ipn.mx/glosario.html
[16] http://firewall.blogcindario.com/2006/05/00003-componentes-de-un-firewall.html
[17] http://www.quadernsdigitals.net/datos_web/hemeroteca/r_1/nr_17/a_213/213.htm

- *Concentra la seguridad*: el firewall facilita la labor a los responsables de seguridad, dado que su máxima preocupación de encarar los ataques externos y vigilar, mantener un monitoreo.
- *Control y estadísticas*: permite controlar el uso de Internet en el ámbito interno y conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas.
- *Choke-Point*: permite al administrador de la red definir un (embudo) manteniendo al margen los usuarios no-autorizados fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques.
- *Genera Alarmas de Seguridad*: el administrador del firewall puede tomar el tiempo para responder una alarma y examina regularmente los registros de base.
- *Audita y registra Internet*: permite al administrador de red justificar el gasto que implica la conexión a Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda.

1.4.3. CLASIFICACIÓN FIREWALLS[18]

Los firewalls se puede clasificar según su característica como:

Modelo de arquitectura

Dependiendo del lugar donde se coloquen en la red pueden tener distintas funciones. Cuando hay dos o más firewalls implementados en una red, estos se comunican con Internet u otras redes recibiendo el nombre de firewall de contención, en cambio el que se encuentra situado internamente y protege redes internas se le denomina firewall bastión.

Firewalls de software y hardware

Entre los firewalls de software se encuentra VPN-1/Firewall-1 de Checkpoint, Iptables, ISA server de Microsoft. En hardware están PIX de Cisco, Netscreen de Juniper Networks.

Teniendo en cuenta que existen soluciones de firewalls de software integrados con aplicaciones como IP-Nokia/Firewall-1, Crossbean/firewall-1, etc. Estas soluciones se clasifican en:

[18] http://www.informatica-hoy.com.ar/seguridad-informatica/Tipos-de-firewall.php

- Firewalls Software
  - ✓ Soportados por varios Sistemas Operativos.
  - ✓ Soportados en varias plataformas.
  - ✓ Productos Mixtos.
- Firewalls Hardware
  - ✓ Hardware – Aplicación + Software preinstalado.
  - ✓ Sistemas operativos Fabricantes
  - ✓ Funcionalidades añadidas como VPN, cache.
  - ✓ Disco duros

Firewall de host y Firewalls de red

Los firewalls host protege los sistemas donde están instalados, y los de Red protegen el entorno de la red o redes donde se han implementados.

- Firewall red
  - ✓ Protegen redes enteras
  - ✓ Sistemas dedicado a la función de Firewall
  - ✓ Módulos adicionales como IDS/IPS, antivirus
  - ✓ Más caros
- Firewall hosts
  - ✓ Firewalls personales.
  - ✓ Embebidos en Sistemas operativos.
  - ✓ Sistemas de conexión externa a través de VPN
  - ✓ Baratos.

2. HERRAMIENTAS PARA DISEÑO E IMPLEMENTACIÓN FIREWALL/LINUX

Durante la realización de diseño e implementación de un servidor/firewall con Linux en esta monografía se necesitará distribuciones de Linux.

2.1. ¿QUÉ ES GNU/LINUX?[19]

GNU/Linux es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux, que es usado con herramientas de sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU) y otra serie de licencias libres.

Para este proyecto de implementar un Servidor/Firewall en una máquina designada, se ha escogido unos distro libre y gratuitos que ayudara a gestionar este proceso. La distribución "ClarkConnect 5.0 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.
La distribución de Linux Kubutu es una distribución GNU/Linux derivada de Ubuntu, que usa el entorno de escritorio KDE (el cual es más configurable) en lugar del GNOME que usa Ubuntu.
Además de la aplicación para firewall Firestarter que es uno de los cortafuegos más sencillos de utilizar y configurar que podemos encontrar para GNU/Linux.

2.2. GNU/LINUX CLARKCONNECT COMMUNITY 5.0

ClarkConnect es un software para servidor de puerta de enlace gateway basado en sistema operativo Linux, con acceso simultáneo a Internet para múltiples usuarios con una sola conexión sobre líneas dedicadas, incluye un completo módulo de administración con todas las optimizaciones necesarias aprovechando los recursos de hardware disponibles.

2.2.1. REQUERIMIENTOS MÍNIMO PARA LA INSTALACIÓN DEL GNU/LINUX CLARKCONNECT

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.

[19] http://www.hispalinux.es/GNULinux

Nota: el servidor ClarkConnect no necesita teclado ni monitor después de su instalación y configuración. El servidor necesita obligatoriamente 2 tarjetas de red para su funcionamiento.

HARDWARE BASE	
Procesador / CPU	Hasta cuatro procesadores - Pentium®, Celeron®, AMD Athlon®
Memoria RAM	Como mínimo se recomienda 512 MB
Disco Duro	Como mínimo se recomienda 1 GB de almacenamiento
Unidad Óptica / CD-ROM	Se requiere únicamente para la instalación
Tarjeta de video	Cualquier tarjeta de video
Tarjeta de Sonido	No es requerida
PERIFÉRICOS	
Mouse	No es requerida
Monitor y Teclado	Sólo requerido para la instalación
RED	
Conexión a Internet (Broadband)	Ethernet, banda ancha , DSL o conexión wireless
Tarjetas (adaptadoras de red)	PCI, ISA o PCMCIA Wireless

Tabla 1. Requerimientos para la instalación del S.O ClarkConnect

Para instalar y configurar 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 Institucional u Organizacional, el usuario tiene completa libertad para hacerlo.

2.2.2. PASOS A SEGUIR PARA LA INSTALACIÓN DEL GNU/LINUX CLARKCONNECT COMMUNITY EN UN SERVIDOR

Qué se necesita para poder instalar un GNU/Linux ClarkConnect Community Edition 5.0:

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.

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 Community Edition 5.0.

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.

2.2.3. INSTALACIÓN Y CONFIGURACIÓN CLARKCONNECT COMMUNITY

En esta sección notara como se realiza la instalación del ClarkConnect Community Edition 5.0 paso a paso.

Es necesario poder arrancar (“bootear”) el servidor por CD-ROM. Si esta opción no está habilitada, en las opciones de la BIOS 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 "*Press 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 [Av. 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.

Fig. 1. Instalación ClarkConnect 5.0

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 servidor. En nuestro caso nos interesa instalar el ClarkConnect, así que escribimos *Linux* y presionamos [*Enter*].
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).

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.
- 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*] seleccionara nuestra elección.

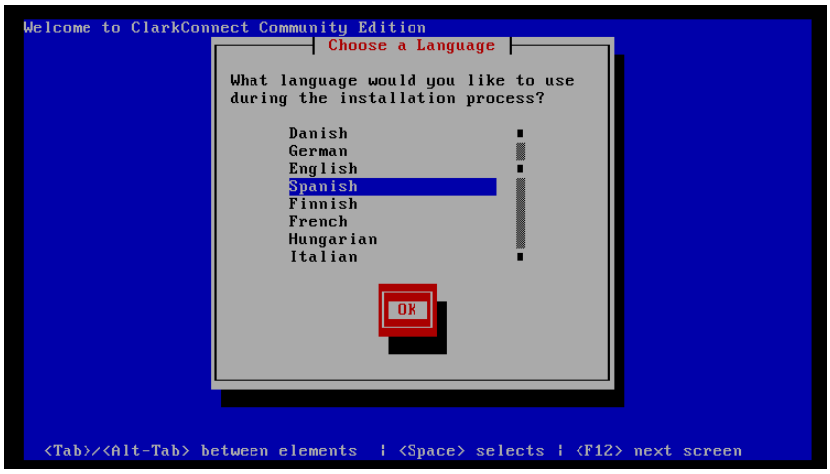


Fig. 2. Selección de idioma de la instalación

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. Es recomendable dejar el lenguaje en inglés, ya que, sólo una pequeña porción del asistente, de instalación al igual que la interfaz Web, se encuentran traducidos al español. Esto ayuda a evitar confusiones con los idiomas.

Fig. 3. Selección de idioma del teclado.

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

Fig. 4. Selección método de instalación

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.

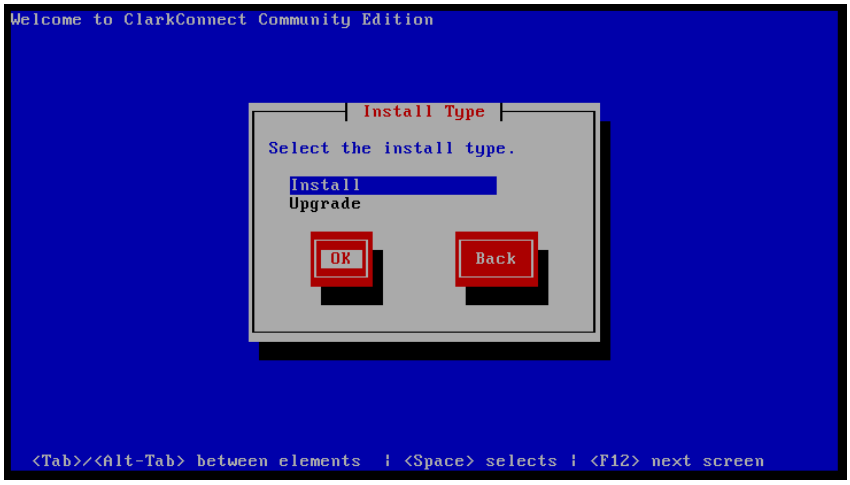


Fig. 5. Selección tipo de instalación

Deseamos instalar así que seleccionamos Install.

Fig. 6. Borrado y/o instalación del S.O.

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

Fig. 7. Selección modo del sistema

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 todos los módulos y posibilidades que nos trae el ClarkConnect Community Edition 5.0 y lo más importante: filtrará el contenido y nos protegerá la LAN.

Fig. 8. Selección tipo de conexión

Llegamos a la sección donde debemos seleccionar qué tipo de conexión a Internet tenemos. Dado que la conexión en la cual trabajaremos es Ethernet, seleccionamos esta.

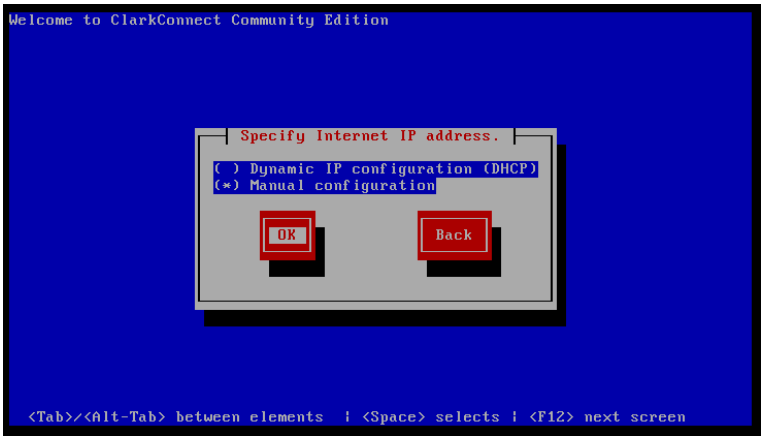


Fig. 9. Especificación direccionamiento IP de Internet

En este paso se especificara que tipo de configuración IP de red se utilizara. Dynamic IP configuration (DHCP) para asignar de manera automática las direcciones IP de la red, Manual configuration se debe conocer las direcciones IP de la red o consultar con el administrador de red, cual es la configuración apropiada.

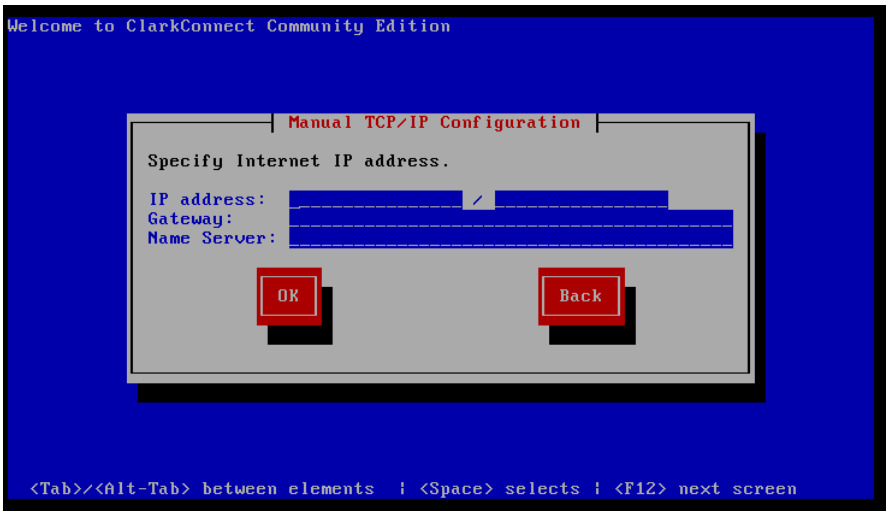


Fig. 10. Configuración Internet IP address

Configuramos la dirección IP pública o la otorgada por el proveedor de servicios de Internet, la máscara de red (Network Mask); si es necesario, también escribir el nombre o la dirección de IP del servidor DNS primario (Name Server).

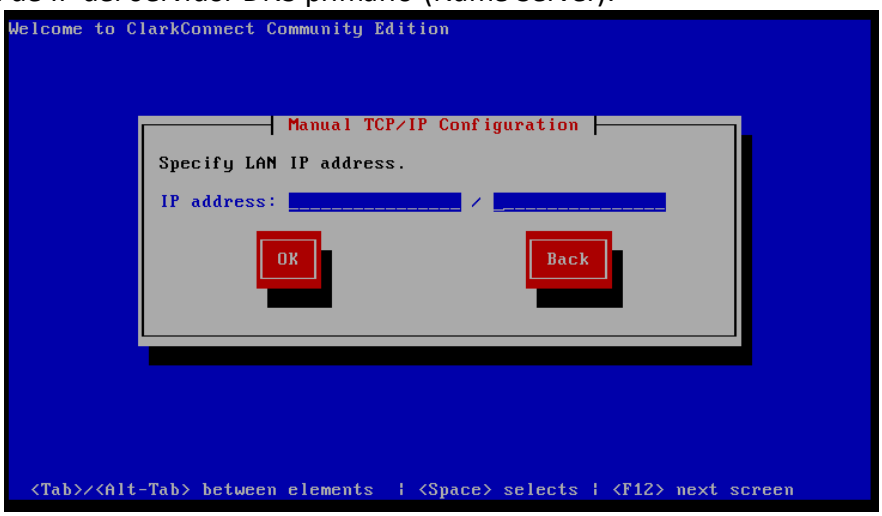


Fig. 11. Configuración LAN IP address

Terminando de configurar la parte de la red, escogemos qué dirección IP tendrá nuestra red LAN y mascara de red. 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.

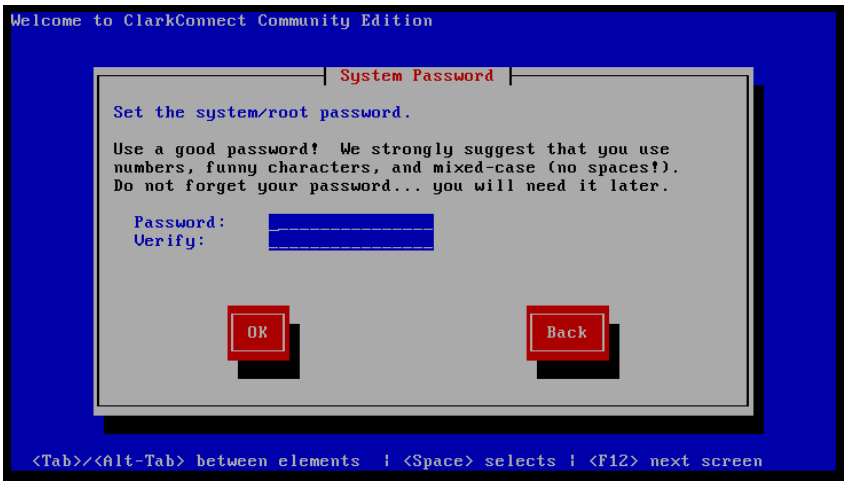


Fig. 12. Configuración contraseña del sistema

Ahora, continuando con la siguiente pantalla, el manual nos pide ingresar una contraseña para el Superusuario (root) en el servidor. Es mejor aceptar la sugerencia que nos hacen de usar números, caracteres especiales (ej.: @#$%&), 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, se recomienda tener una contraseña de mínimo 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 arriba y obtener algo así:

Ejemplo: *Mi contraseña secreta*
----------> M&c0ntr@$enn@$ekret4

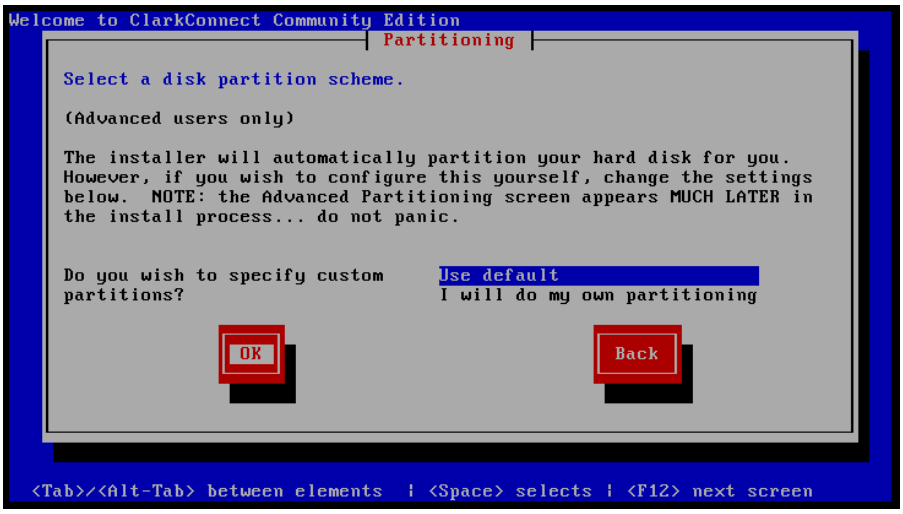


Fig. 13. Selección para partición de Disco duro

Llegamos ahora a la sección más crítica 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.

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. 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 más 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.

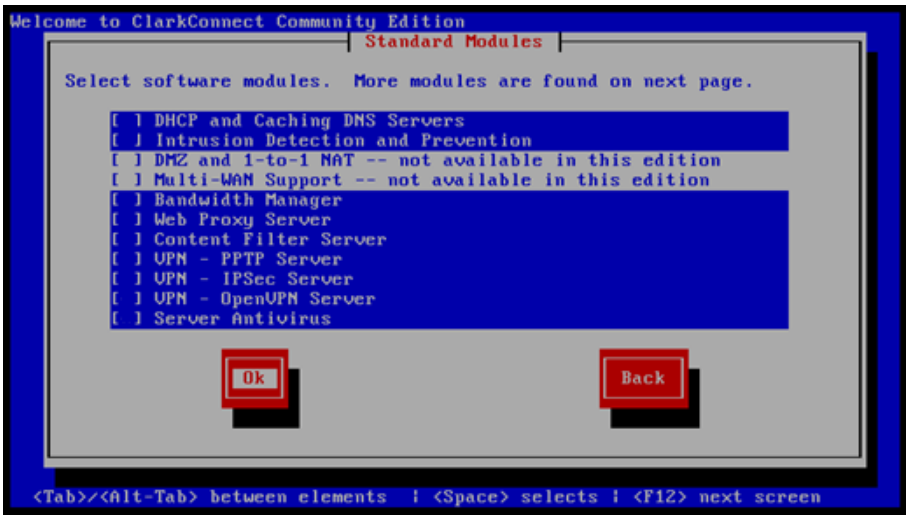


Fig. 13.1 Módulos para firewall ClarkConnect

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

A continuación explicaremos brevemente cada módulo:

DHCP 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 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, entre otros.

VPN – 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.

VPN – OpenVPN Server: servidor VPN privado que proporciona road warrior VPN. OpenVPN es más robusto en el paso de otros cortafuegos y entrada.

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

Para el Servidor/Firewall necesitaremos los módulos de *DHCP, Bandwidth Manager, Web Proxy Server, Content Filter Server y Server Antivirus*; 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; si se desean otras posibilidades para realizar con el servidor, como por ejemplo compartir archivos, sólo basta con seleccionar el módulo 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.

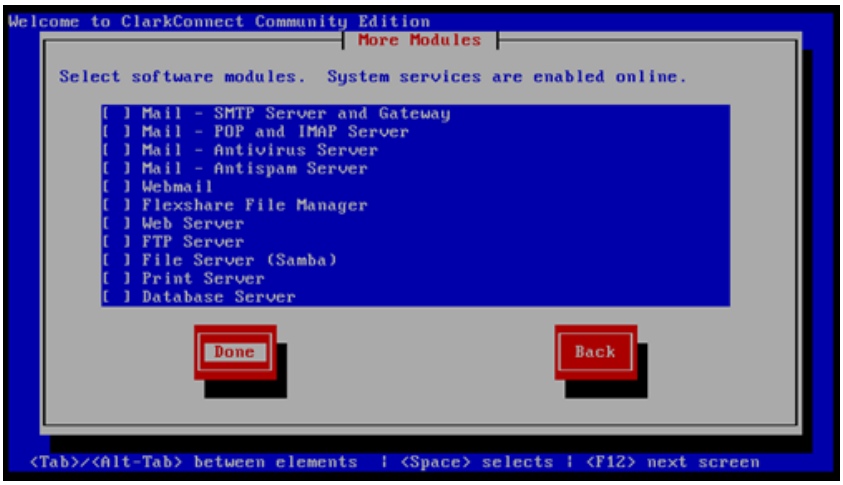


Fig. 14. Módulos de servicios

Mail – SMTP Server and Gateway: módulo para administrar un servidor de correo electrónico propio. Posee control de SPAM y de virus.

Mail - POP and IMAP 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 (HTTP/HTTPS), FTP (FTP/FTPS), File Shares (Samba) 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.

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 "administrable" desde una interfaz Web.

Al seleccionar los módulos deseados presionamos *Done.*

Fig. 15. Confirmación correcta de la configuración S.O

¡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.

En esta etapa comienza a correr el instalador del ClarkConnect. Sólo basta esperar mientras se instala y carga todos los archivos necesarios para el Servidor/Firewall.

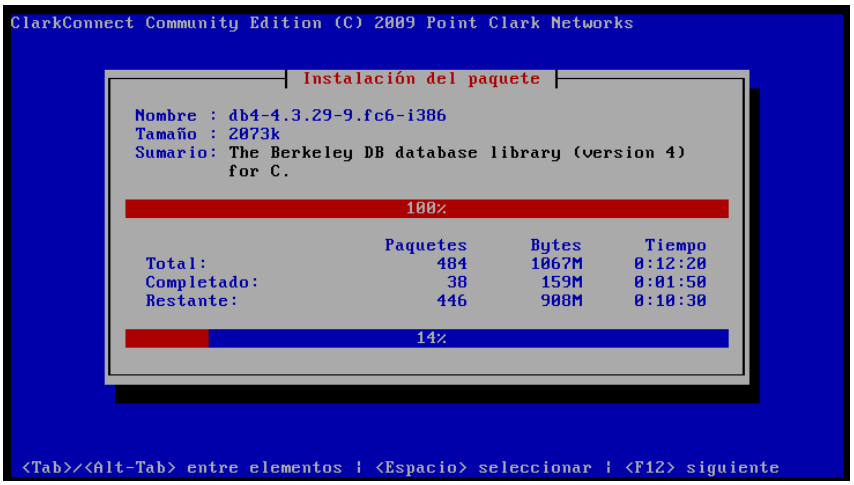


Fig. 16. Instalación de paquetes

Minutos después de comenzar con la instalación, nos muestra un último mensaje.

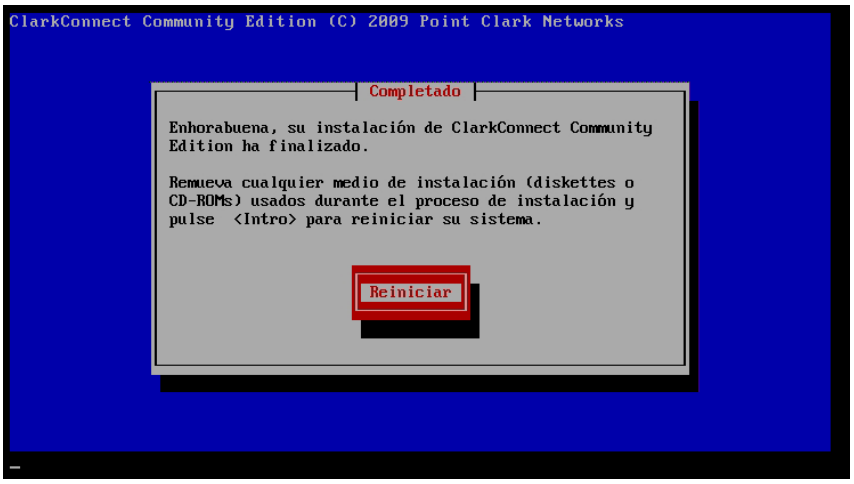


Fig. 17. Finalización y reinicio del S.O.

Ahora que la instalación está completa procedemos a retirar el CD-ROM y a reiniciar el computador (presionando [*Enter*]).

2.2.4. POST-INSTALACIÓN

Acabamos de instalar el ClarkConnect Community Edition 5.0 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.

Fig. 18. Inicialización de S.O ClarkConnect

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.

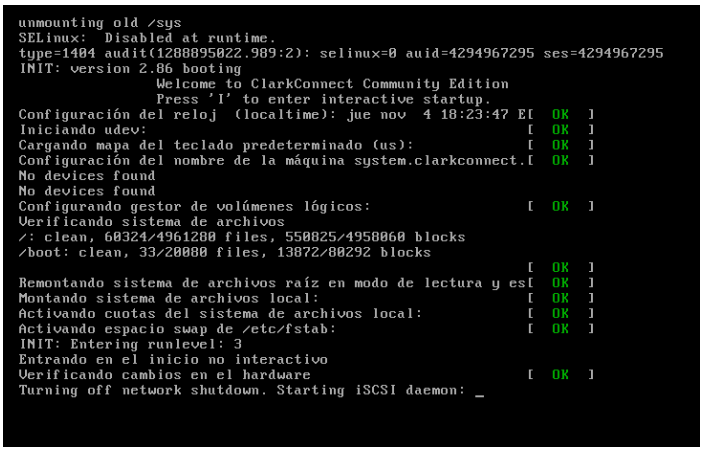


Fig. 19. Carga de archivos de inicio del sistema archivos S.O.

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.

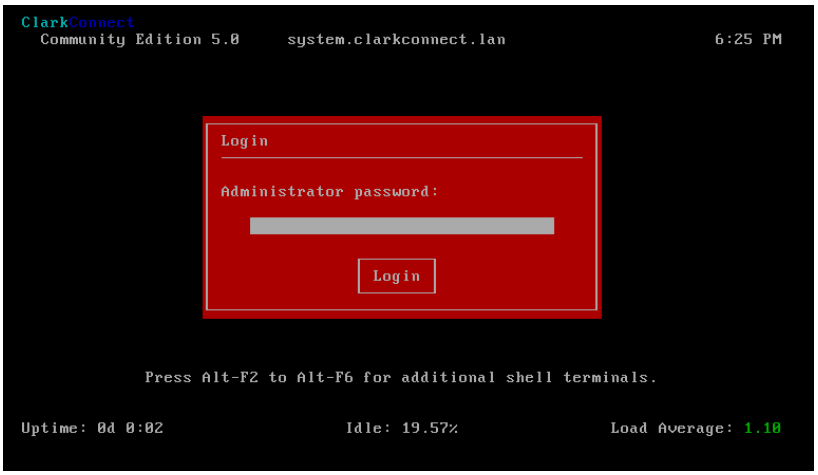


Fig. 20. Log In, Ingreso al sistema

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 F1) nos puede ser muy útil y fácil de usar.

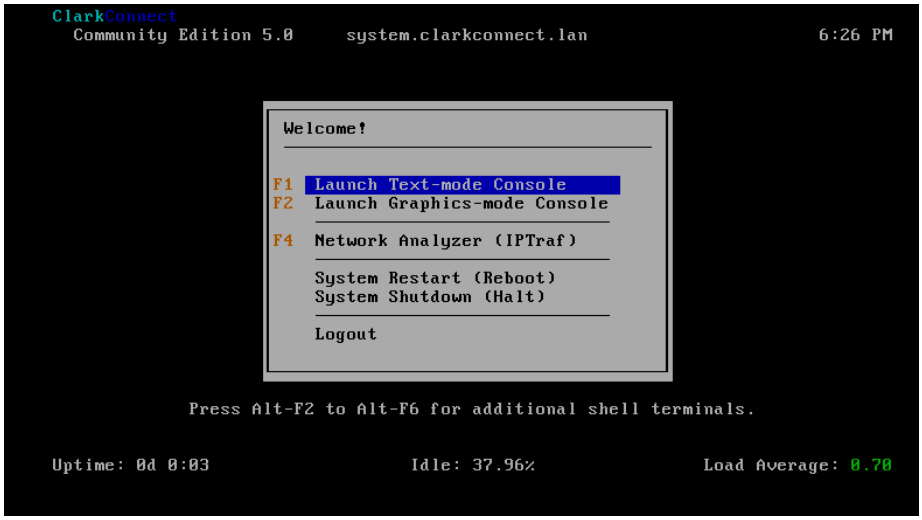


Fig. 21. Menú de inicio S.O. ClarkConnect

Cuando termine de cargar escribimos [F1] 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.

2.2.5. INTERFAZ WEB, INGRESO

De ahora en adelante para administrar el servidor se necesita un computador conectado a la red local, Colocar la dirección IP la cual coloco en la red. En nuestro caso la: 192.168.1.2

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

Fig. 22. Selección panel de control de Windows

1. Seleccionar Panel de Control desde el menú de Inicio.

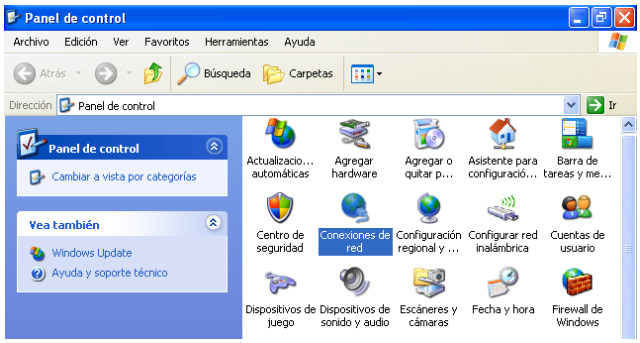


Fig. 23. Selección Conexiones de red

2. Hacer clic en Conexiones de Red desde el Panel de Control.

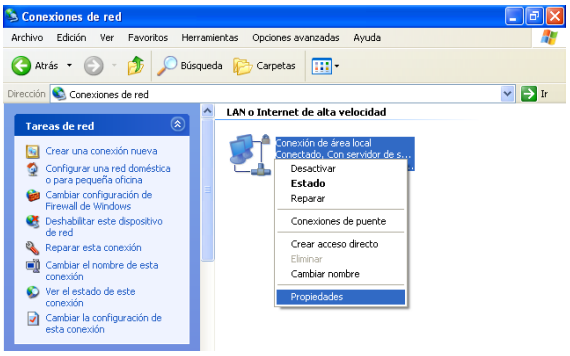


Fig. 24. Selección propiedades conexión de red

3. Escoger la conexión de la red LAN y Clic en Propiedades.

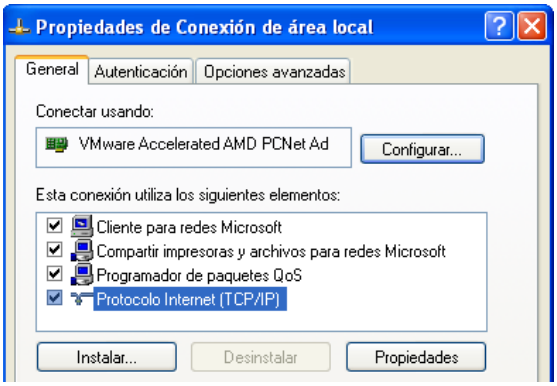


Fig. 25. Selección propiedades Protocolo de Internet (TCP/IP)

4. Seleccionar Protocolo de Internet (TCP/IP) con un doble clic o presionar en el botón propiedades.

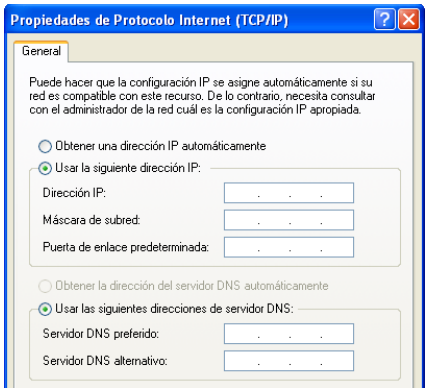


Fig. 26. Propiedades protocolo de Internet (TCP/IP)

Se selecciona Usar la siguiente dirección de IP y escribimos lo siguiente:

- Dirección de IP: 192.168.1.3 (los últimos dígitos puede ser cualquier número dentro del rango del 1-253).
- Mascara de Subred: 255.255.255.0
- Puerta de enlace: 192.168.1.2, esta es la dirección de IP del servidor.

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 5 se escoge automática en ambas secciones.

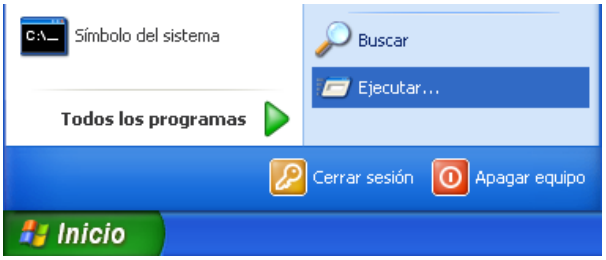


Fig. 27. Abrir aplicación *Ejecutar*

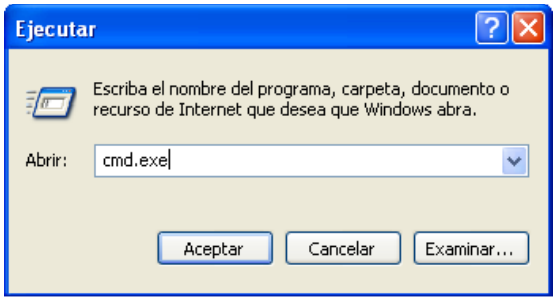


Fig. 28. Ejecutar aplicación Símbolo del sistema

Realizado esto se abre una consola en ejecutar, luego escribir: cmd.exe

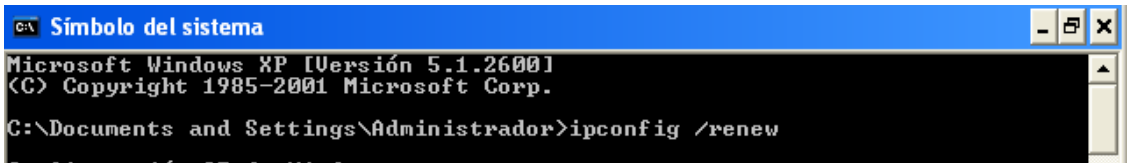


Fig. 29. Comando ipconfig

Se digita ipconfig /renew y esto actualizará la IP de la máquina por una que provee el servidor en el rango especificado.

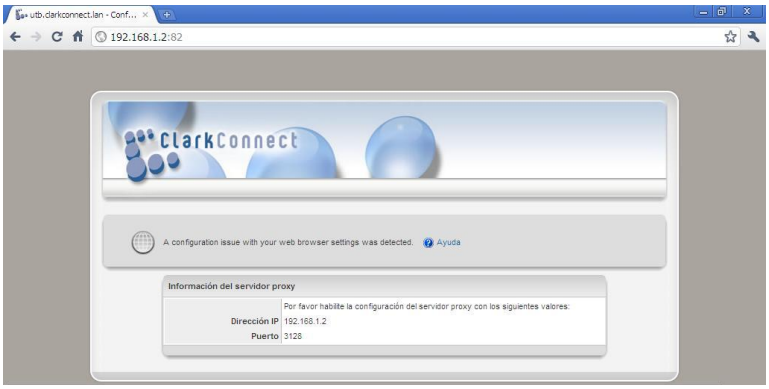


Fig. 30. Interfaz web ClarckConnect

Abrimos un navegador y escribimos https://192.168.1.2:82 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 192.168.1.2 y por el puerto 82. (Los servidores Web comunes usan el puerto 80 como estándar para comunicarse, pero para evitar confusiones y problemas de seguridad, en el ClarkConnect el servicio de la interfaz Web se encuentra en el puerto 82).

2.2.6. CONFIGURACIÓN INTERFAZ WEB CLARKCONNECT COMMUNITY EDITION

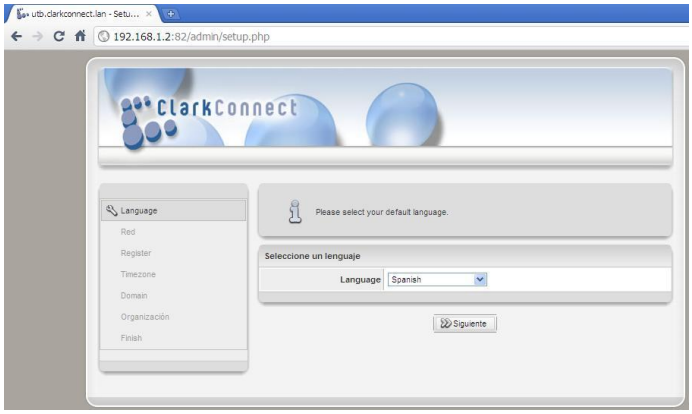


Fig. 31. Configuración lenguaje ClarkConnect

Ya ubicados en el navegador y escribimos https://192.168.1.2:82/admin/setup.php y presionamos [Enter]. Ésta es la dirección para ingresar a la configuración de la interfaz Web del servidor ClarkConnect. Aquí nos pide escoger el idioma de configuración del ClarkConnect.

Fig. 32. Configuración Red ClarkConnect

En este paso se especificara que tipo de configuración IP de red se está utilizando.

Interfaz:

La primera interfaz eth0, este nombre se designa a la primera tarjeta de red, este es el papel que la interfaz desempeña en la red como: interfaz externa, la cual se conecta directamente al Internet. Se pueden utilizar uno de los dos tipos:

1. Dinámico: para conexiones a Internet a través de un módem o cuando se conecta a otro servidor que sirva DHCP.
2. Estática: cuando se le quiere designar al servidor una IP fija, tanto para la LAN como para Internet.

Red:

Se escoge el modo *puerta de enlace*, allí aparecerá las direcciones IP de los servidores DNS.

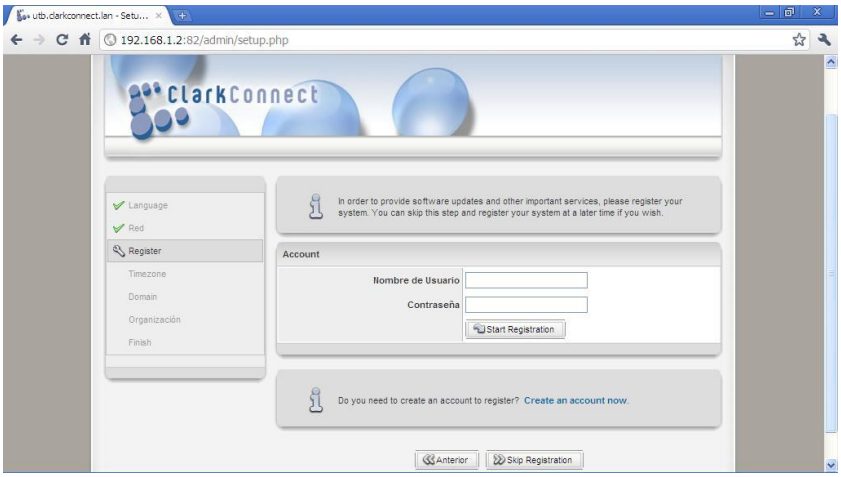


Fig. 33. Configuración Registro ClarkConnect

A continuación nos aparece la ventana para registrar nuestro sistema para el uso de actualización y módulos del ClarkConnect. Si no desea regístralo puede omitir este paso y registrarlo cuando desee.

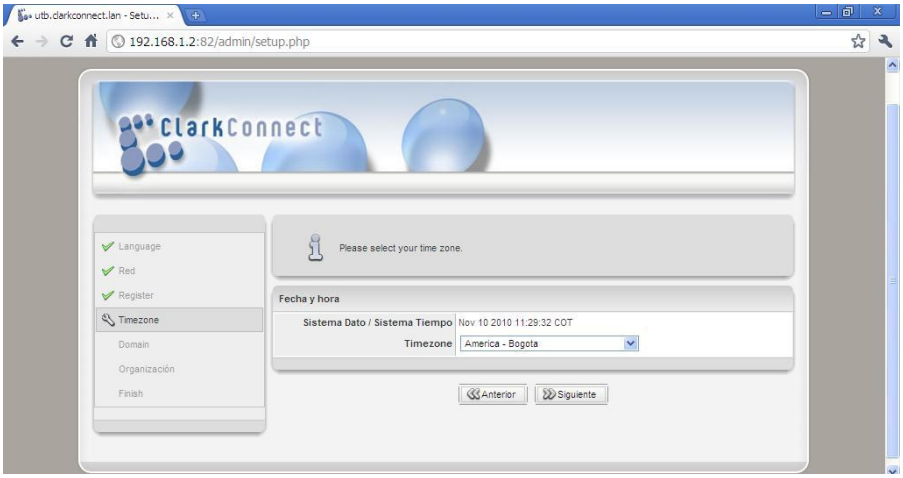


Fig. 34. Configuración zona horaria ClarkConnect

Continuamos seleccionando la zona horaria. En nuestro caso se utilizó *América – Bogotá.*

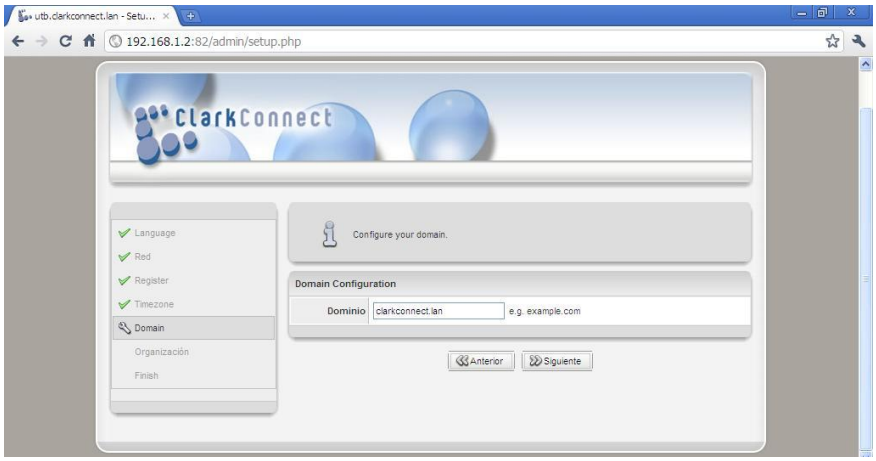


Fig. 35. Configuración del dominio ClarkConnect

En este paso escogerá el dominio el cual desea que se encuentre su red. En nuestro caso se escogió *ClarkConnect.lan.*

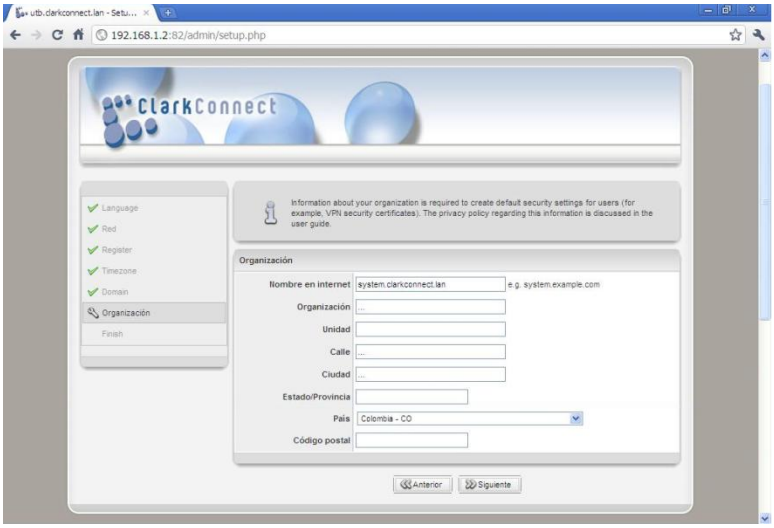


Fig. 36. Configuración de la institución u organización del ClarkConnect

En esta parte se completará la información de la institución u organización. Este tipo de datos es utilizado por ClarkConnect para la seguridad del servidor al momento de actualizarse o descargar módulos.

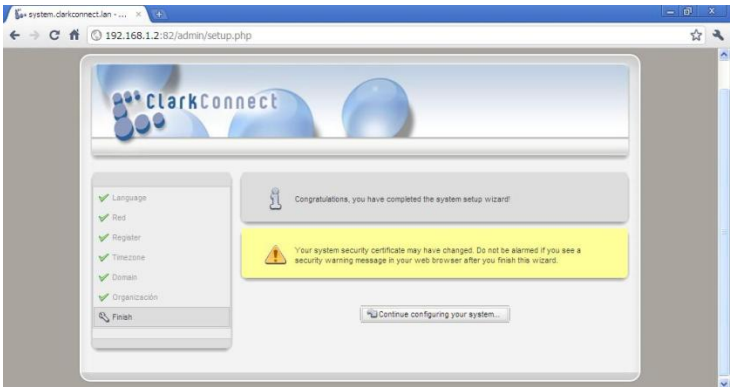


Fig. 37. Finalización Configuración del ClarkConnect

Acabamos de finalizar la etapa de configuración para ingresar a la interfaz Web. Ahora aparece una advertencia y suponiendo que estamos seguros en lo que vamos a hacer presionamos *Continue configuring your system*.

2.2.7. 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.

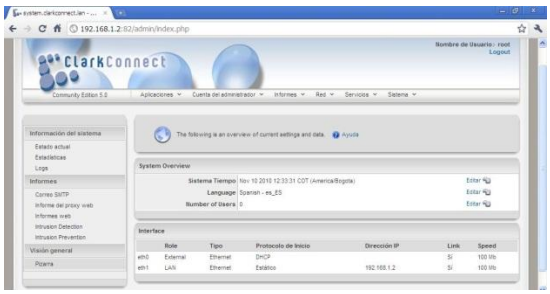


Fig. 38. Configuración final de la red ClarkConnect

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.

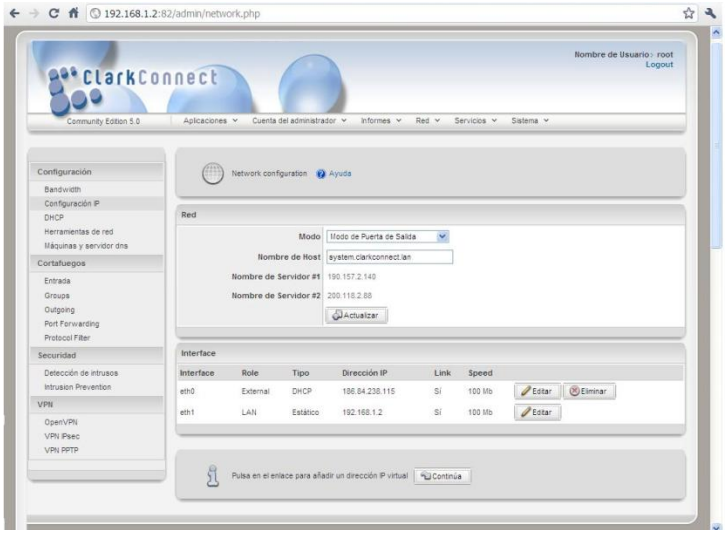


Fig. 39. Configuración IP ClarkConnect

Nos vamos a la pestaña *Red* y seleccionamos *Configuración IP*. 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, seleccionamos Gateway Mode. 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.

En *Nombre del Host* aparece el nombre que le dimos a la máquina junto con la red a la que pertenece, por ejemplo:

ClarkConnect.lan

Éste se puede cambiar de ser necesario a un nombre más 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 *Actualizar*. ¡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 10.5 y 10.5.1. Si es necesario a través de la consola se pueden modificar manualmente estos DNS, esto puede ser muy conveniente para diferentes usos.

2.3. FIRESTARTER, GUI[20] COMO HERRAMIENTA FIREWALL EN LINUX

Firestarter es uno de los cortafuegos más sencillos de utilizar y configurar que podemos encontrar para GNU/Linux. Es una muy buena opción para tener de forma rápida y cómoda un cortafuego que satisfaga la mayoría de nuestras necesidades.

2.3.1. PASOS A SEGUIR PARA LA INSTALACIÓN DE LA APLICACIÓN FIREWALL FIRESTARTER

Para la instalación de la aplicación firewall Firestarter de manera sencilla, necesitamos que nuestro equipo tenga instalado un sistema operativo Linux para este documento se utilizara la distribución Kubuntu 10.04 LTS (**Ver anexo 1**) y que esté conectado a la Internet para poder descargar el paquete de instalación y proceder con el proceso de instalado.

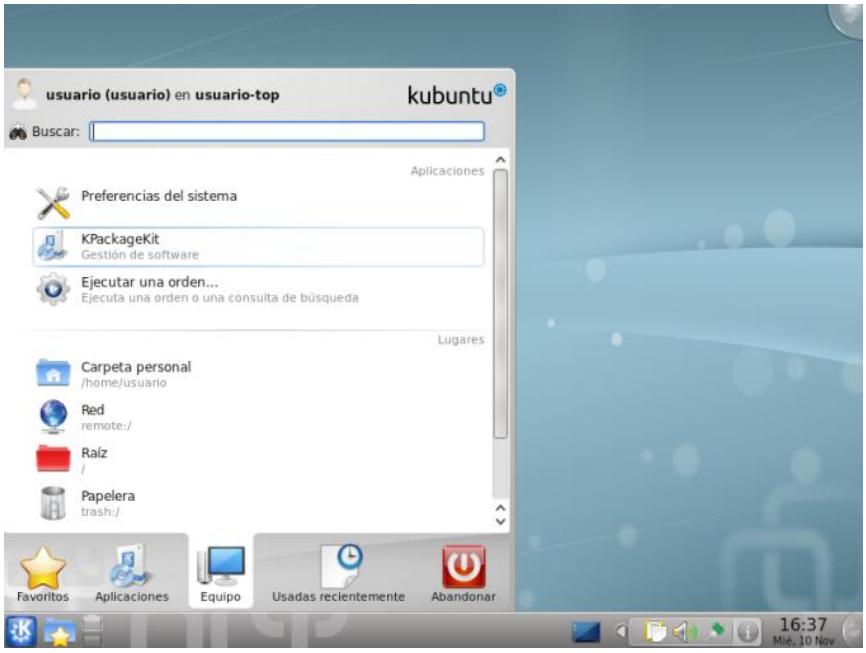


Fig. 40. Gestor de software - KPackageKit (búsqueda Firestarter)

Desde el menú de KDE (kickoff) Equipo → KPackageKit

[20] Graphical User Interface: interfaz gráfica de usuario

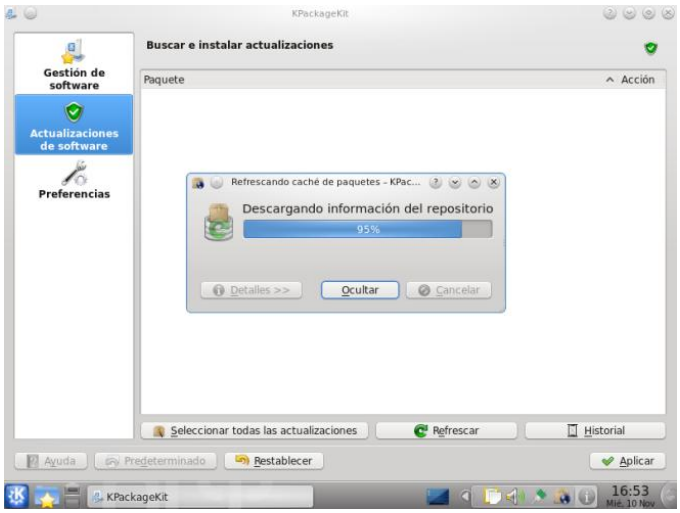


Fig. 41. Actualización repositorio KPackageKit

Con la aplicación ejecutada, nos dirigimos a la opción actualizar software. Para así actualizar el cache de paquetes (aplicaciones) de Linux.

Para instalar una aplicación o paquete específico lo haremos de la siguiente forma:

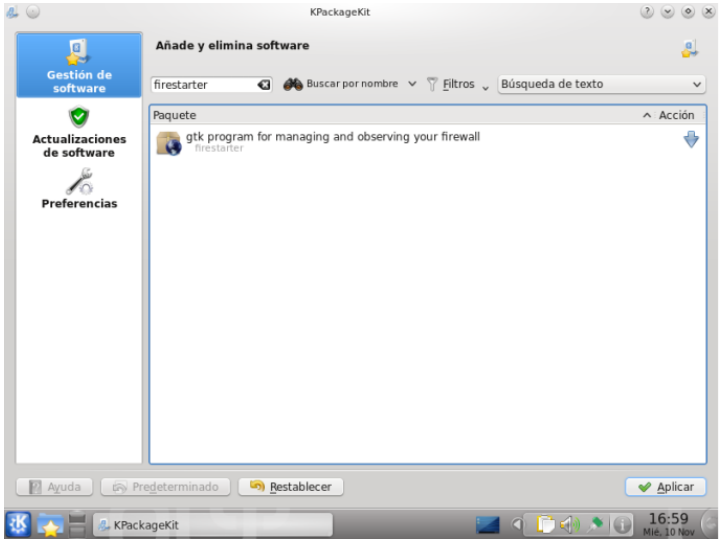


Fig. 42. Búsqueda paquete de instalación Firestarter

Introducimos en el cuadro de texto "*Buscar paquetes*" el nombre de la aplicación firewall la cual necesitamos instalar y pulsamos [Enter]. En este caso instalaremos la aplicación Firestarter.

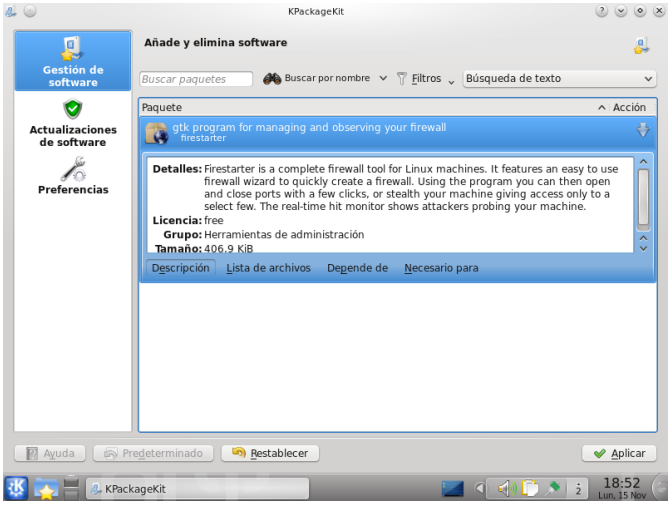


Fig. 43. Detalle del paquete de instalación Firestarter

Haz clic en el paquete deseado y podrás ver una descripción del mismo así como diferentes pestañas por las cuales navegar y ver otros detalles del paquete.

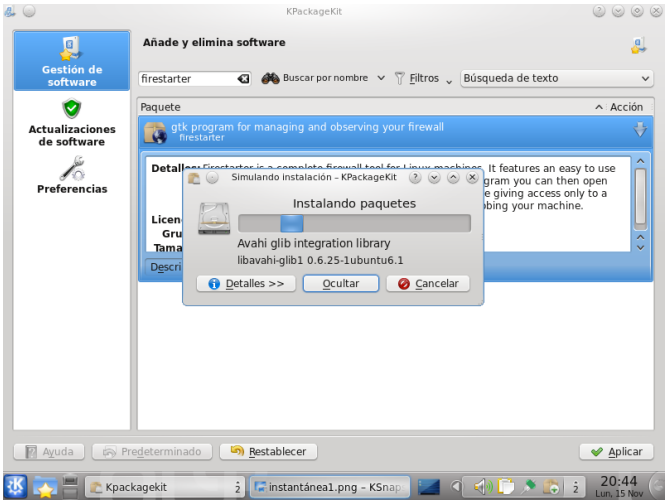


Fig. 44. Simulación instalación paquete Firestarter

Pulsa en el pequeño icono de una flecha hacia abajo y verás como que se ilumina. Después haz clic en el botón [*Aplicar*] y te saldrá un diálogo de simulación de la instalación del paquete.

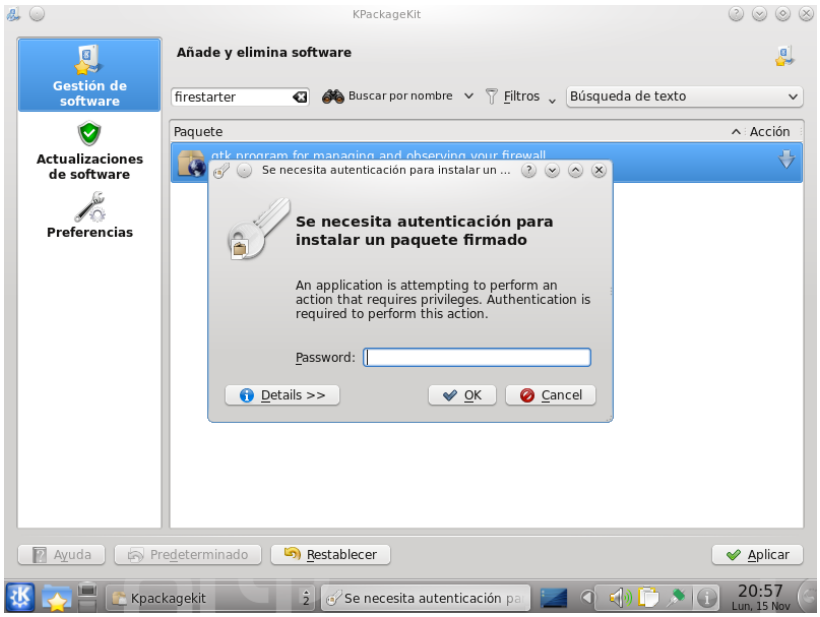


Fig. 45. Autenticación para la instalación Firestarter

El sistema operativo exigirá la contraseña de autenticación (contraseña inicio de sesión).

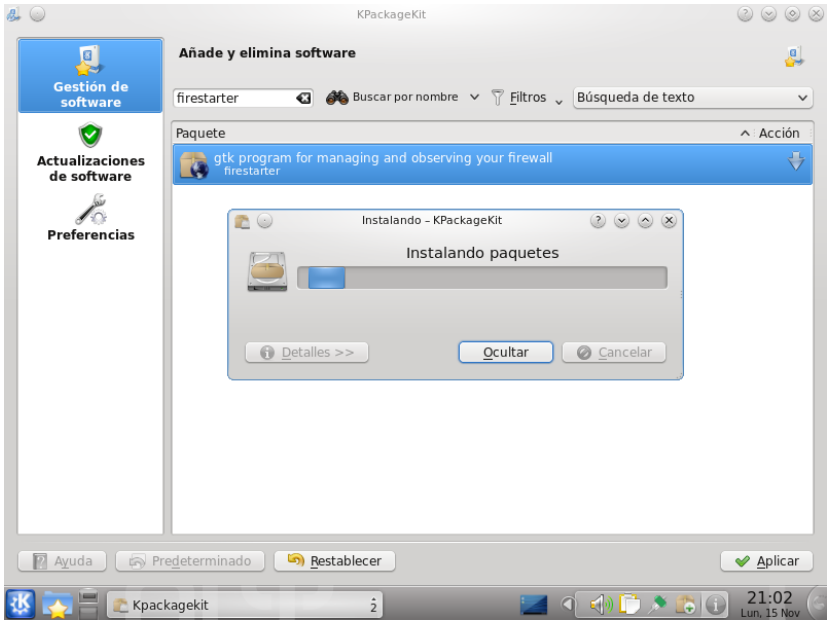


Fig. 46. Instalación de paquetes de instalación Firestarter

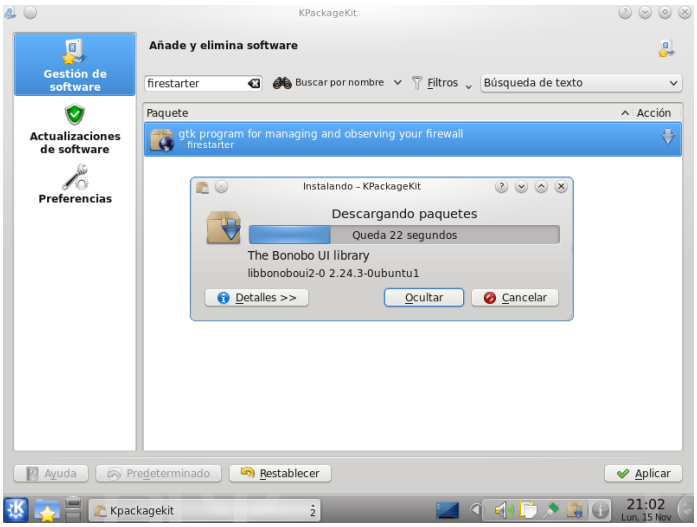


Fig. 47. Descarga de paquetes de instalación Firestarter

Luego de colocada la contraseña para comenzar a descargar e instalar el paquete. **¡Listo!** Una vez que termine ya tendrás la aplicación instalada y cerramos el gestor de software KPackageKit.

2.3.2. ASISTENTE DE CONFIGURACIÓN DE LA APLICACIÓN FIREWALL "FIRESTARTER"

Explicaremos cómo configurarlo para permitir el tráfico a través de un puerto con un par de ejemplos.

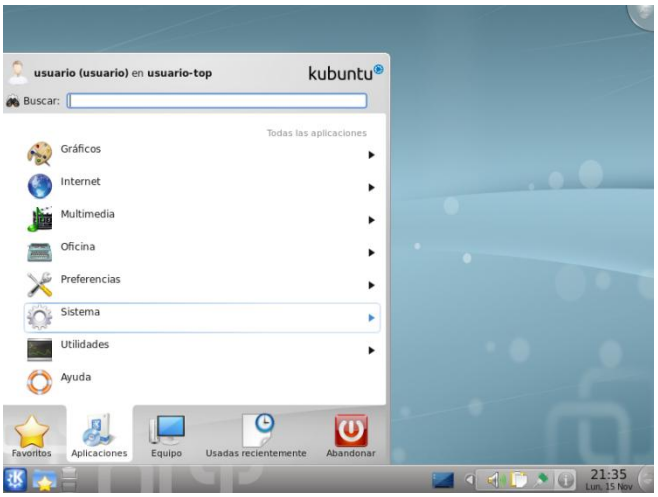


Fig. 48. Menú de aplicaciones Kubuntu 10.04 GNU/LINUX

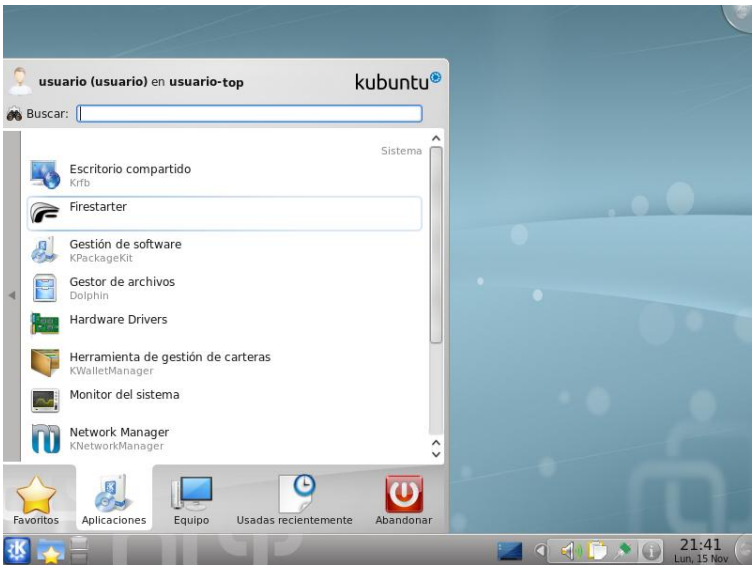


Fig. 49. Menú de sistema Kubuntu 10.04 GNU/LINUX

Desde el menú de KDE (kickoff) Aplicaciones → Sistema → Firestarter

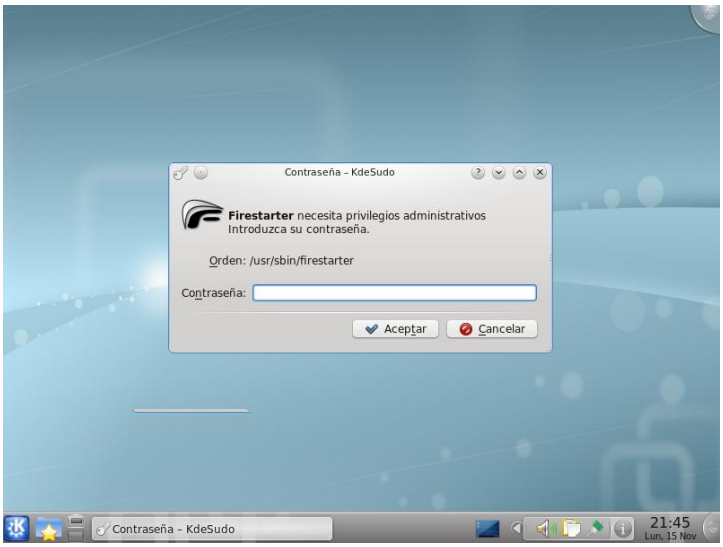


Fig. 50. Autenticación del sistema para abrir Firestarter

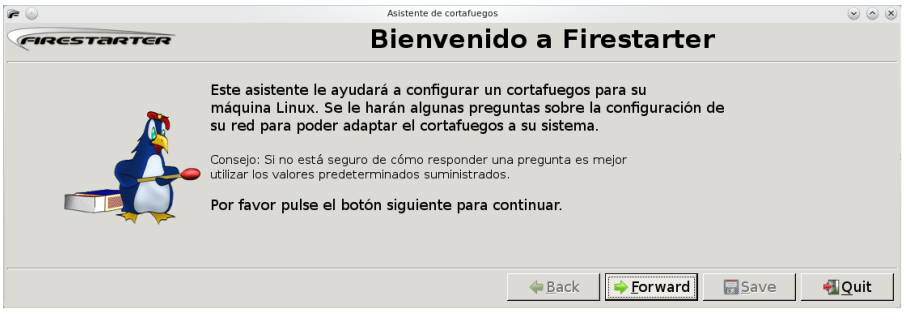


Fig. 51. Asistente de bienvenida Firestarter

La primera vez que iniciemos Firestarter Kubuntu nos pedirá la contraseña de privilegios de administrador, posteriormente se nos abrirá un asistente que nos configurará los parámetros básicos del cortafuegos. Pulse siguiente «Forward».

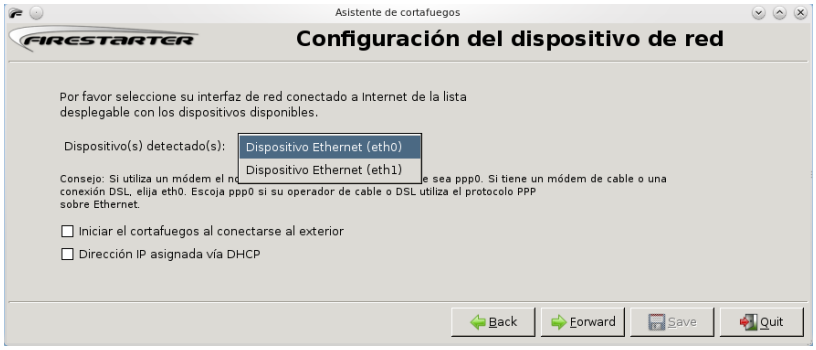


Fig. 52. Configuración de dispositivos de red Firestarter

En esta ventana configuraremos la interfaz conectada a Internet, el asistente detectará automáticamente todas la interfaces de red, deberemos seleccionar la que está conectada directamente a Internet, en nuestro caso ha detectado dos tarjetas de red.

También tenemos dos opciones cuyas casillas podemos marcar dependiendo de nuestro tipo de conexión.

Iniciar el cortafuego al conectarse al exterior: Si no tenemos conexión directa, podemos usar esta opción para que el cortafuego no esté operativo si no estamos conectados, así mismo se reiniciará en caso de que perdamos la conexión y volvamos a reconectar, ya sea manualmente o automáticamente.

Dirección IP asignada vía DHCP: Si nuestra conexión se configura de este modo, marcando esta casilla esta conexión estará permitida por defecto, pero siempre podemos dejarla

desmarcada y permitir esta conexión creando una regla que solo permita la conexión a nuestro servidor DHCP.

Escogido cada uno de los parámetros pulse siguiente «Forward».

Fig. 53. Configuración conexión Internet Firestarter

Como se quiere compartir la conexión o recursos entre los PCs, podemos activarla desde esta ventana. Lógicamente debemos de disponer de más de una interfaz de red y la seleccionada en esta ventana debe de ser diferente a la que seleccionamos en la ventana anterior.

En este paso solamente marcaremos la casilla "Activar la compartición de la conexión a Internet" si queremos que nuestro servidor sea el que hace de servidor de DHCP y el provee Internet a los demás ordenadores de nuestra red. En el caso, que se esté utilizando un router y/o un switch para la conexión a Internet, no se necesita utilizar un PC como proxy, aunque es recomendable para instalar un filtro de contenido web gratuito para la navegación por Internet, o como cortafuegos de nuestra conexión. . Pulse siguiente «Forward».

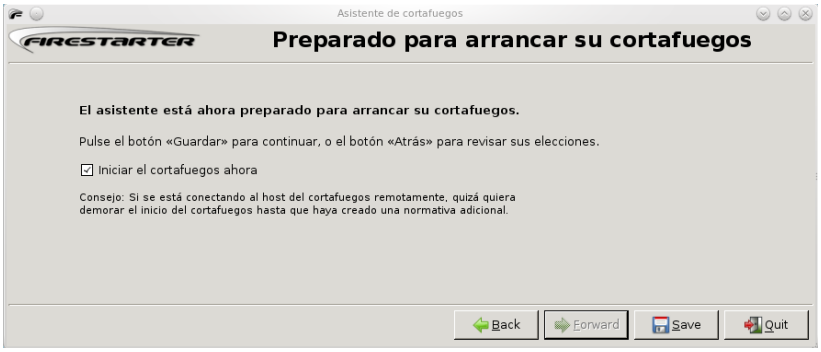


Fig. 54. Finalización del asistente Firestarter

A continuación nos da la posibilidad de iniciar el cortafuego ahora, en este punto hay que proceder con precaución pues si estamos configurando Kubuntu de forma remota (con VNC, con escritorio remoto, etc.) al marcar esta opción nos cortará la conexión. Si estamos configurándolo de forma local (en el Servidor) podremos activarlo sin problemas. Pulsamos guardar «Save» para continuar con la configuración de Firestarter.

2.3.3. CONFIGURANDO EL CORTAFUEGO FIRESTARTER

Fig. 55. Ventana principal Firestarter

Llegaremos a la pantalla principal de Firestarter en la tenemos las tres pestañas desde las que se administra este cortafuego:

- Estado: Muestra el estado del cortafuegos.
- Eventos: Muestra las conexiones que el cortafuegos ha rechazado.
- Normativa: Muestra las reglas que hemos definido para configurar el cortafuegos.

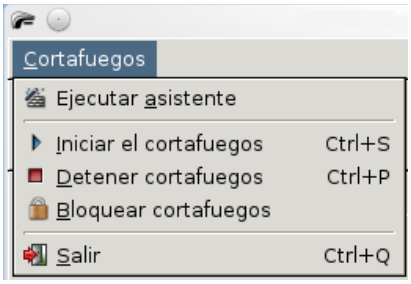


Fig. 56. Menú Cortafuegos Firestarter

Desde los correspondientes iconos, podemos Detener el cortafuego, lo cual permitirá todas las conexiones, o Bloquear el cortafuego, lo cual detendrá todo el tráfico. Las funciones de Estado y el Asistente se encuentran en el menú Cortafuegos.

Algunas de las preferencias no tienes mayor importancia, pero otras si influyen en la configuración del cortafuegos.

Interfaz:

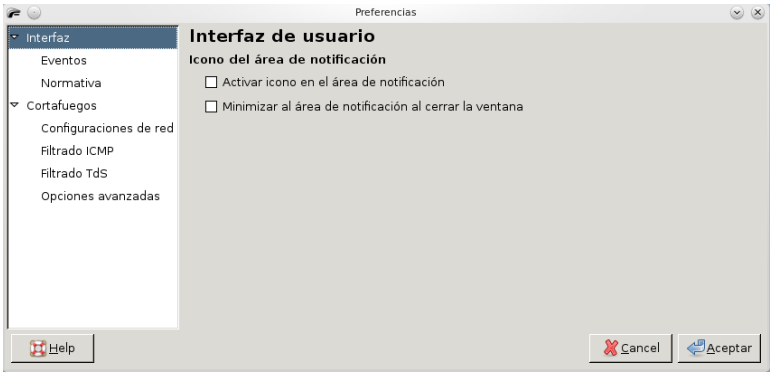


Fig. 57. Preferencias Firestarter

Activar icono en el área de notificación: Coloca un icono de notificación la bandeja del sistema. Este icono muestra el estado del cortafuego y parpadea cuando se registra algún evento. Si pinchamos sobre el icono, se abrirá y cerrará la ventana principal del programa.
Minimizar al área de notificación al cerrar la ventana: Al salir el programa no se cerrará si no que se minimizará en el icono de notificación.

Eventos:

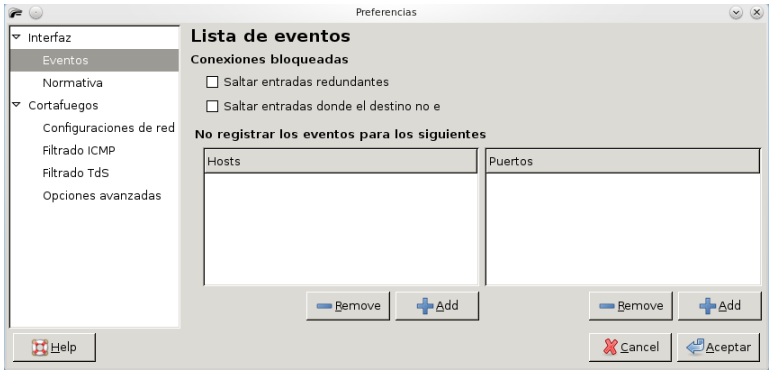


Fig. 58. Eventos Firestarter

Saltar entradas redundantes: Marcando esta pestaña no se listarán en la pestaña "Eventos" las conexiones bloqueadas que sean consecutivas e idénticas.

Saltar entradas donde el destino no es el cortafuego: No se listarán las conexiones bloqueadas cuya dirección IP de destino no sea la misma que la del cortafuego, generalmente mensajes de Broadcasting.

No registrar los eventos para los siguientes: En esto recuadros, añadiremos/quitaremos a mano, mediante sus correspondientes botones, las direcciones o puertos que no queremos sean listados en "Eventos". Las direcciones o puertos se pueden incluir automáticamente desde la lista de eventos como veremos en la correspondiente sección.

Directivas:

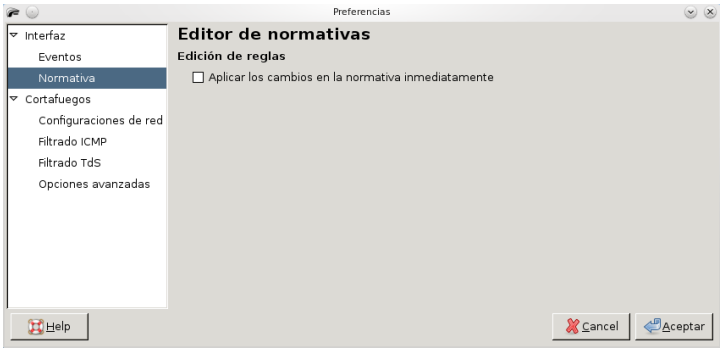


Fig. 59. Normativa Firestarter

Aplicar los cambios en la directiva inmediatamente: Los cambios se aplican sin necesidad de usar el botón "Aplicar".

Cortafuegos:

En estas secciones se pueden controlar funciones más avanzadas del cortafuego, junto con algunas configuraciones que ya se realizaron mediante el asistente.

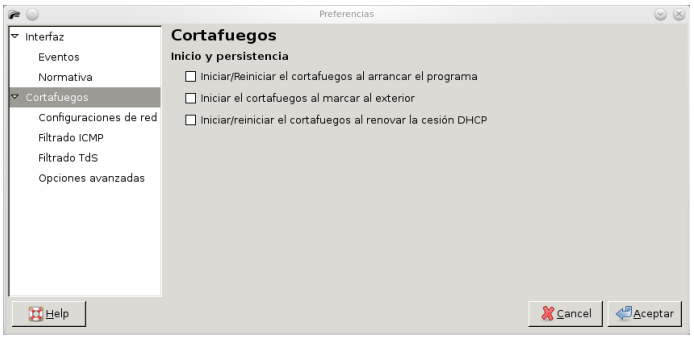


Fig. 60. Cortafuego Firestarter

- ❖ Iniciar/reiniciar el cortafuegos al arrancar el programa.
- ❖ Iniciar el cortafuego al marcar al exterior.
- ❖ Iniciar/reiniciar el cortafuegos al renovar la cesión DHCP

Configuraciones de red:

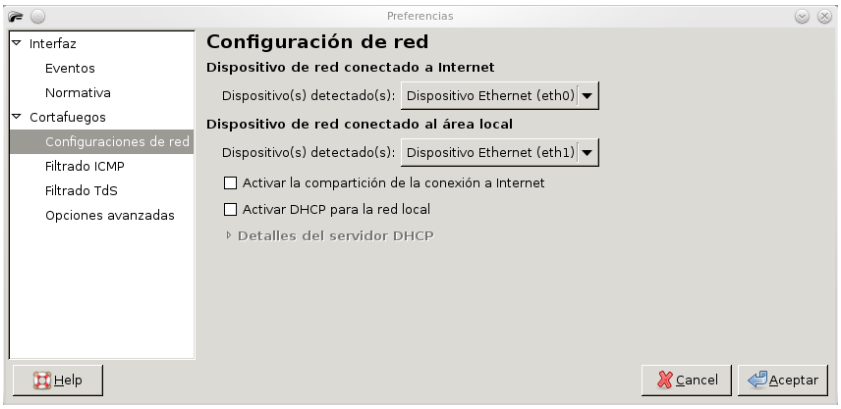


Fig. 61. Configuración de red Firestarter

Filtrado ICMP:

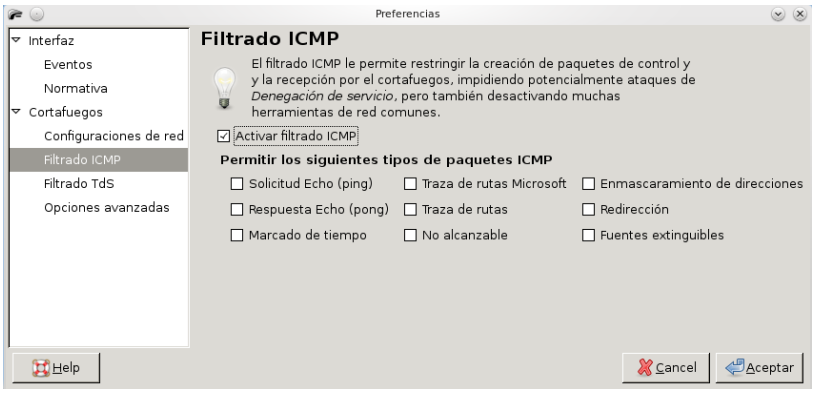


Fig. 62. Filtrado ICMP Firestarter

Desde aquí podemos bloquear todos los ICMP activando el filtrado, pudiendo también selecciona mediante la casilla correspondiente algunos de ellos si fuera necesario.

Filtrado TdS (Tipo de Servicio):

Fig. 63. Filtrado TdS Firestarter

Este tipo de priorización debe de estar soportado por la red a la que nos conectamos, lo que en la práctica limita el área de efecto a redes locales.

Opciones avanzadas:

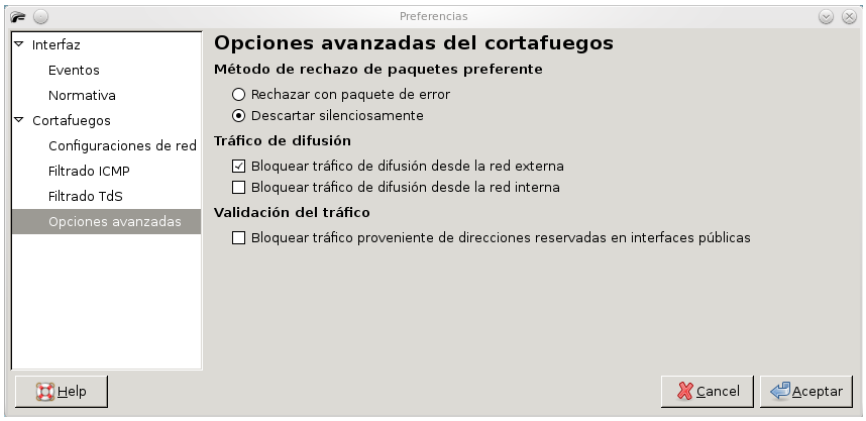


Fig. 64. Opciones avanzadas Firestarter

Método de rechazo de paquetes preferente: Podemos elegir entre que los paquetes se rechacen con un mensaje de error (puerto cerrado/closed) o en silencio (puerto bloqueado/invisible/stealth).

Tráfico de difusión: Podemos bloquear desde aquí todo el tráfico de difusión (Broadcasting).

2.3.4. CONFIGURACIÓN PARA CONEXIÓN DE RED LAN

Si se tiene dirección IP pública o la otorgada por el proveedor de servicios de Internet, la máscara de red (Network Mask); si es necesario el nombre o la dirección de IP del servidor DNS primario (Name Server). Deberá seguir los pasos que se realizaran para la conexión a la red LAN.

Nota: La primera tarjeta nos indica la conexión a Internet.

Fig. 65. Verificación conexión a Internet SO

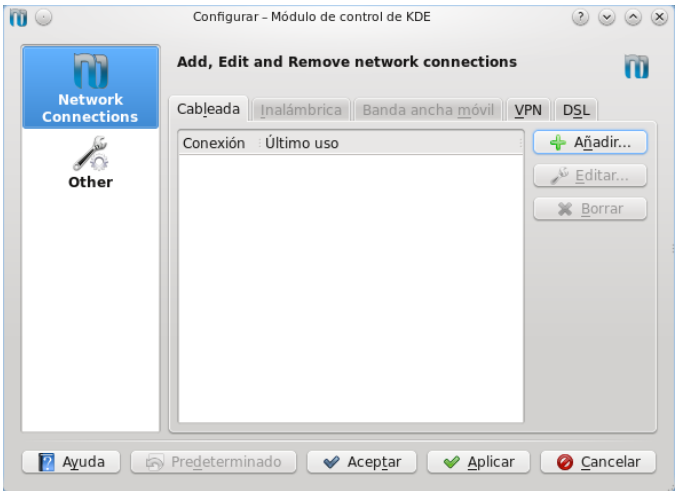


Fig. 66. Gestor de conexiones de red

Realizamos clic en el icono que aparece en la imagen y nos dirigimos a *Gestionar las conexiones…*, posteriormente nos dirigimos al botón añadir para colocar las configuraciones que tendrá la interfaz Ethernet para la red LAN.

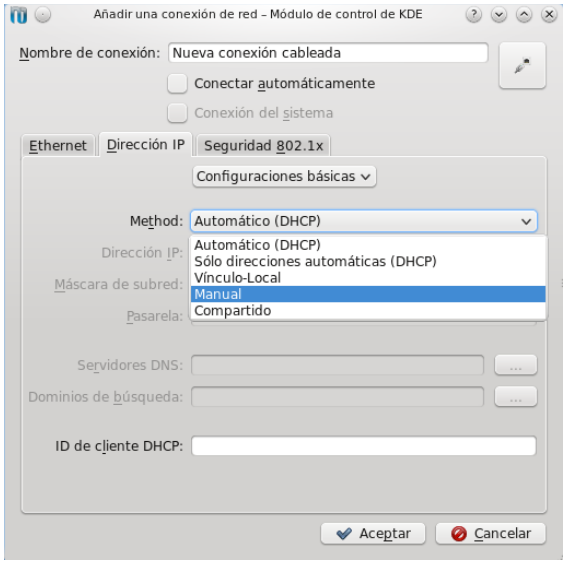


Fig. 67. Configuración manual Interfaz Ethernet de la red

Existen varios métodos para configurar la interfaz Ethernet de la red LAN:

- Automático (DHCP)
- Solo direcciones automática (DHCP)

- Vinculo-Local
- Manual
- Compartido

En este manual se tomara el método manual para la configuración de la red.

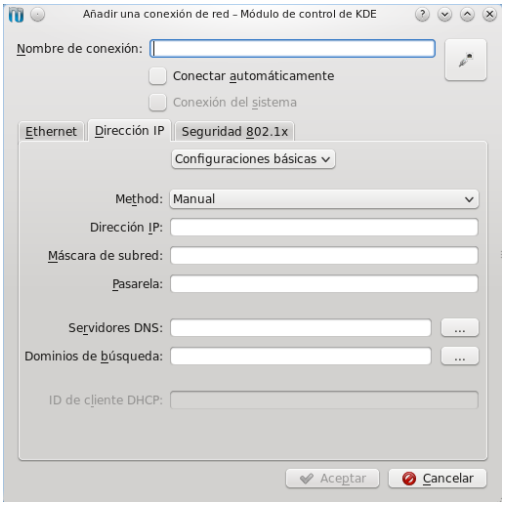


Fig. 68. Ingreso de datos de la interfaz Ethernet de la red

Escogemos qué dirección IP tendrá nuestra red LAN y mascara de red. 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, Colocamos mascara de subred, puerta de enlace (pasarela). Ingresado todos los datos finalizamos en *Aceptar*.

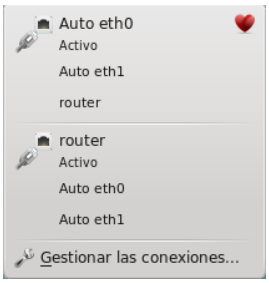


Fig. 69. Verificación de interfaces Ethernet de la red

Terminada la configuración de la interfaz Ethernet LAN, aparecerá el nombre de la conexión y la indicación activo.

2.3.5. CREANDO REGLAS PARA ABRIR PUERTOS

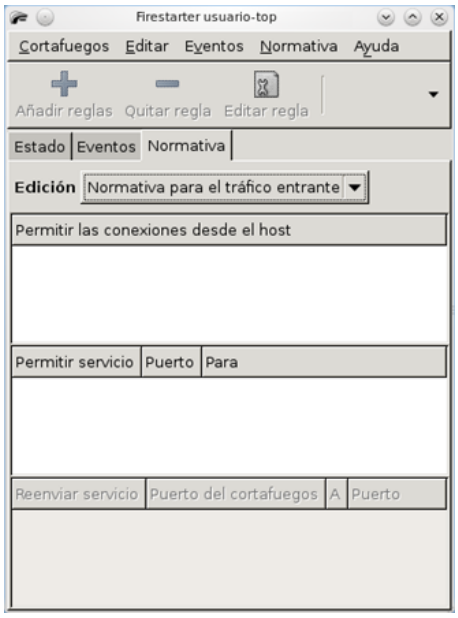


Fig. 70. Configuración de reglas del Firestarter

Como lo que queremos es configurar las reglas necesarias para que el cortafuego permita el acceso a través de ciertos puertos, iremos a la pestaña Normativa para crear nuestras reglas personalizadas.

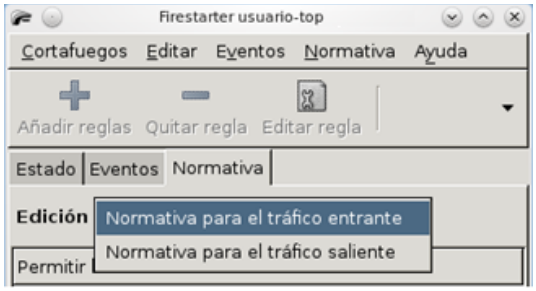


Fig. 71. Configuración de reglas trafico entrante del Firestarter

Para crear nuestras reglas, primero dejaremos seleccionada la opción *Normativa para el tráfico entrante.*

La *normativa de tráfico saliente* la tocaremos más adelante, ya está controlara todo el tráfico de nuestra máquina al exterior.

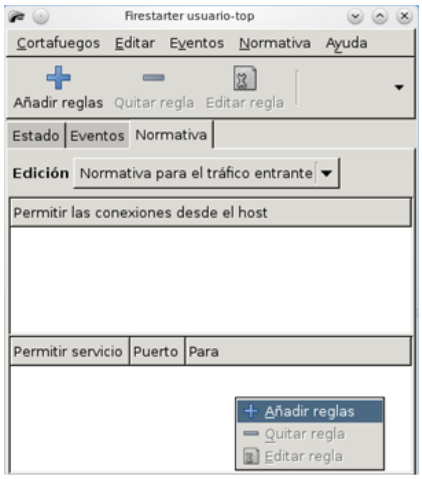


Fig. 72. Añadiendo reglas trafico entrante del Firestarter

Una vez seleccionada esa opción, pincharemos con el botón derecho en el panel inferior, y en el menú contextual que se nos abrirá, seleccionaremos la opción Añadir regla.

Fig. 73. Ejemplo de regla de tráfico entrante del Firestarter (Puerto MSN 1863)

Se nos abrirá una ventana en la que introduciremos la información del puerto que queremos abrir:

Nombre: Nombre descriptivo para el puerto que abriremos.
Puerto: Puerto a abrir (si queremos abrir un rango, pondremos algo del estilo: 6881-6889).
Origen: Si queremos abrirlo sólo para lo que provenga de una IP concreta. Normalmente querremos dejar esta opción en cualquiera.
Comentario: Un comentario (opcional) que describa para qué se usa ese puerto.

Una vez introducidos los datos, le damos al botón Añadir y la regla quedará aplicada.

2.3.6. PERMITIR EL TRÁFICO DE NUESTRA RED

Como el firewall por defecto es muy restrictivo, seguramente nos rechazará la mayoría de tráfico que proviene de nuestra red local. Si se quieren compartir ficheros entre ls máquinas, etc., es posible que queramos configurar una regla para permitir el acceso a nuestra máquina desde los PCs de nuestra LAN.

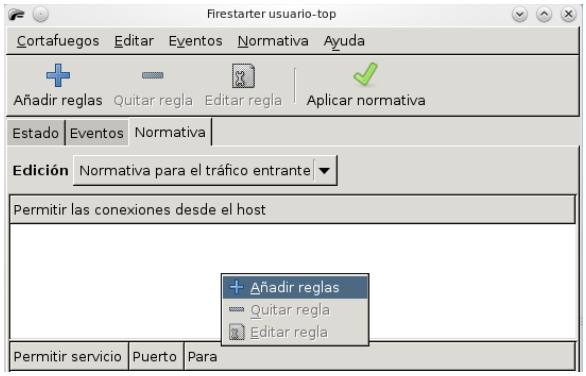


Fig. 74. Permitiendo trafico entrante del Firestarter a la red

Iremos a la pestaña Normativa y pincharemos con el botón derecho del ratón en el recuadro Permitir las conexiones desde el host (teniendo seleccionada en el estado la opción de Normativa para el tráfico entrante).

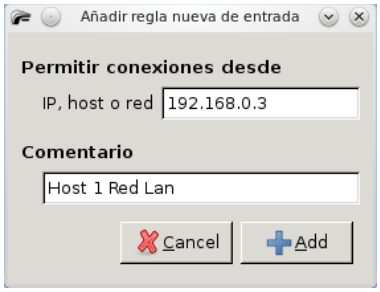


Fig. 75. Ejemplo permitiendo tráfico entrante del Firestarter (IP 192.168.0.3)

En la pantalla que se nos abre podremos introducir la ip, nombre de la máquina o red (ip junto con la máscara) a la que queramos permitir el acceso completo a nuestro PC.

Una vez introducidos los valores (el comentario es opcional), le daremos al botón Añadir. Siguiendo estos pasos pueden configurarse las reglas típicas que necesitaremos en nuestros PCs de escritorio para utilizar las aplicaciones más comunes, y a la vez tener el acceso bien restringido.

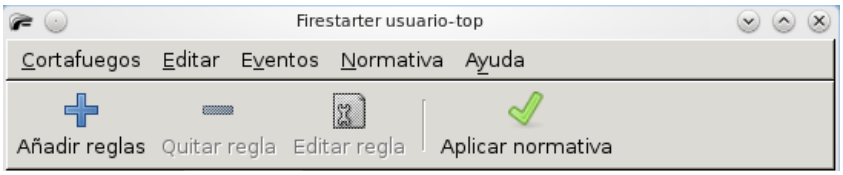


Fig. 76. Aplicando normativas o reglas Firestarter.

Una vez añadidas las direcciones IP deseadas y abiertos los puertos, pulsaremos sobre "Aplicar normativa" para que los cambios tengan efecto.

2.3.7. LA NORMATIVA DE TRÁFICO SALIENTE

El tráfico saliente es generado por un host local y envió a la red. Los datos se generan desde un ordenador en una red local y se envía a un host que se encuentra en la red remota.

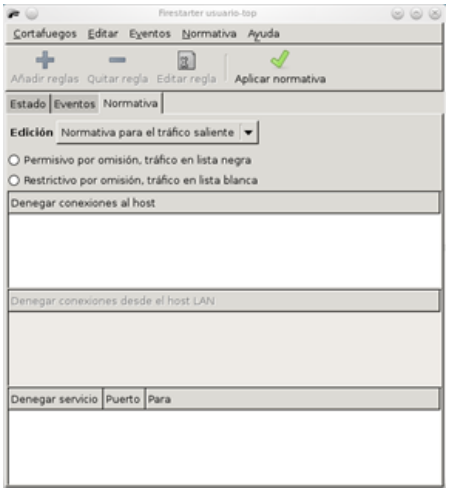


Fig. 77. Normativas trafico saliente Firestarter.

Existen dos políticas diferentes para el tráfico saliente:

- Permisivo: Todo el tráfico saliente está permitido, solo los puertos o direcciones de la lista serán bloqueados.
- Restrictivo: Todo el tráfico saliente será bloqueado, solo el tráfico entre los puertos y direcciones de la lista serán permitidos.

Existen tres tipos de lista para Denegar o Permitir según estemos en modo Permisivo o Restrictivo. En este tutorial se explicaran las 2 primeras opciones.

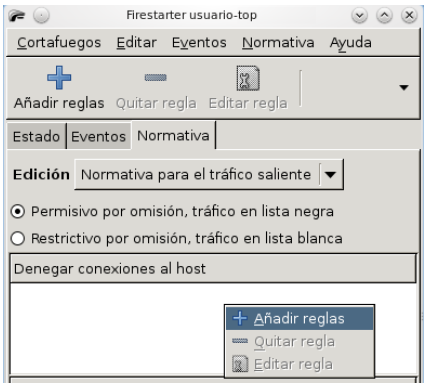


Fig. 78. Añadiendo reglas trafico saliente del Firestarter

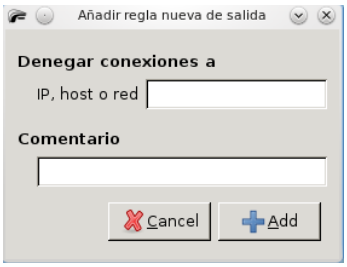


Fig. 79. Añadiendo nueva reglas trafico saliente del Firestarter

Para añadir una regla en alguna de las listas, haremos clic con el botón derecho del ratón en el espacio libre de la lista en la que queramos incluir una regla, ya sea para una dirección IP o una dirección IP de nuestra red.

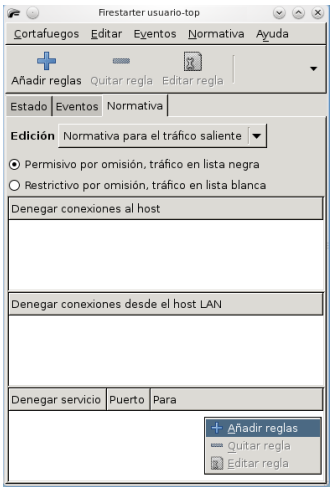


Fig. 80. Añadiendo reglas de servicio trafico saliente del Firestarter

Otra forma de realizar una regla es donde podemos especificar el tipo de servicio/puerto y el origen de la conexión. Haremos clic con el botón derecho del ratón en el espacio libre de la lista en la que queramos incluir una regla.

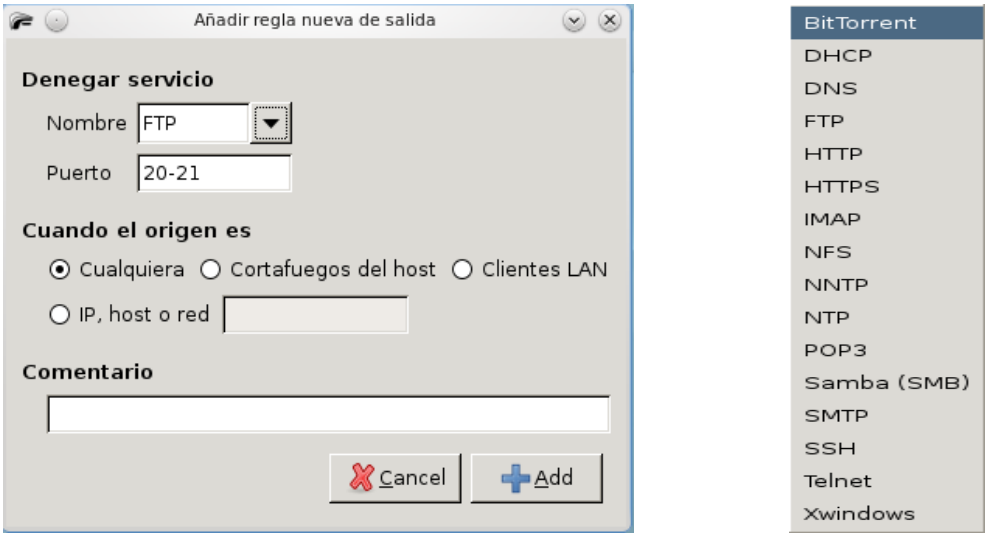


Fig. 81. Ejemplo añadiendo regla denegando servicio ftp del Firestarter

El programa ya trae algunos servicios predefinidos por defecto que podemos seleccionar desde el menú desplegable "Nombre".

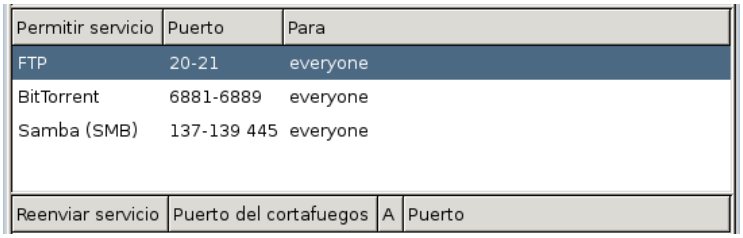
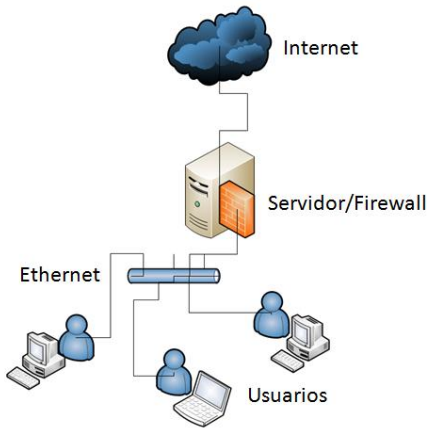


Fig. 82. Ejemplo nombres predefinidos para normativa Firestarter

Las distintas listas con reglas para cada modo son guardadas independientemente de que cambiemos de un modo a otro, porque podemos tener perfectamente configurado tanto el modo Restrictivo como el Permisivo y cambiar de una configuración a otra si así lo necesitamos.

3. IMPLEMENTACIÓN DE PRÁCTICAS

Para la implementación de estas prácticas se usará una arquitectura de host de doble acceso.



En esta arquitectura la red se protegerá perimetralmente por un solo Firewall, que protege la red interior de la red exterior en este caso típico de conexión a Internet y que tiene instalada dos tarjetas de red. La primera tarjeta de red se utilizara para la conexión a la Internet y la segunda tarjeta de red tiene como objetivo realizar la conexión LAN entre el servidor y los demás dispositivos de red.

A continuación se muestra la tabla de direccionamiento IP:

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MASCARA DE RED	GATEWAY
Servidor/Firewall	Fa 0/0	Dir. IP publica[21]	255.255.255.0	---
	Fa 0/1	192.168.1.2	255.255.255.0	Dir. IP Publica[16]
PC 1	N/A	192.168.1.3	255.255.255.0	192.168.1.2
PC 2	N/A	192.168.1.4	255.255.255.0	192.168.1.2
PC 3	N/A	192.168.1.5	255.255.255.0	192.168.1.2

Tabla 2. Direccionamiento IP

3.1. PRÁCTICA 1: BLOQUEO DE DOMINIO (LISTA NEGRA) CLARKCONNECT.

Antes de realizar la práctica debemos conocer cómo se conecta ClarkConnect a la Internet, las direcciones IP usadas y el DNS (**ver sección 2.2.3. y 2.2.5.**). Es necesario conocer este

[21] Esta dirección Ip es proporcionada por quien brinda el servivio ISP (Empresa que brinda el servicio de Internet)

paso, así se tendrá mejor conocimiento de cómo bloquear un domino. En nuestro caso se utilizaron los dominios www.unitecnologica.edu.co y www.utbvirtual.edu.co

3.1.1. DESCRIPCIÓN DE LA PRÁCTICA

Esta práctica nos permite bloquear un dominio específico. Permitiendo todo el tráfico de salida, a excepción del dominio bloqueado, en nuestro caso los domino eran.

3.1.2. REQUERIMIENTOS

Para la ejecución de esta práctica se necesitan los siguientes módulos:

- *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, entre otros.
- *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.

3.1.3. ELABORACIÓN DE LA PRÁCTICA 1

Desde la ventana principal del ClarckConnect nos dirigimos a *Red > Outgoing.* Esta práctica nos permite bloquear un dominio específico. Permitiendo todo el tráfico de salida, a excepción del dominio bloqueado. A continuación escogemos el modo de tráfico de cómo se muestra a continuación:

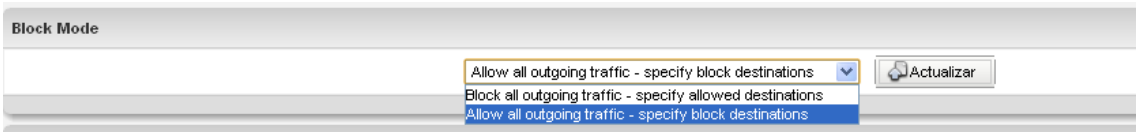


Fig. 83. Selección modo de bloqueo

Si seleccionamos el modo de salida el cual establece que se permita todo el tráfico saliente y bloquee el dominio **www.unitecnologica.edu.co** se podrá navegar por toda la Internet y los usuarios no podrán ingresar al dominio antes mencionado. Para esto ingresamos en la sección de bloqueo de dominios especificando un alias con el cual describiríamos la regla aplicada y el dominio como se muestra a continuación:

Fig. 84. Dominios bloqueados

3.1.4. PRUEBA PRÁCTICA 1

Al momento de realizar la prueba se puede observar que el explorador web no carga los dominios bloqueados.

Fig. 85 No carga el dominio www.unitecnologica.edu.co

Fig. 86 No carga el dominio www.utbvirtual.edu.co

3.2. PRÁCTICA 2: PERMITIENDO DOMINIOS (LISTA BLANCA) CLARKCONNECT.

Antes de realizar la práctica debemos conocer cómo se conecta ClarkConnect a la Internet, las direcciones IP usadas y el DNS (**ver sección 2.2.3. y 2.2.5.**). Es necesario conocer este paso, así se tendrá mejor conocimiento de cómo bloquear un domino. En nuestro caso se utilizaron los dominios www.unitecnologica.edu.co y www.utbvirtual.edu.co

3.2.1. DESCRIPCIÓN DE LA PRÁCTICA

Esta práctica nos permite que 2 dominios específicos puedan tener acceso vía web teniendo en cuenta que todo el tráfico está bloqueado.

3.2.2. REQUERIMIENTOS

Para la ejecución de esta práctica se necesitan los siguientes módulos:

- *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, entre otros.
- *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.

3.2.3. ELABORACIÓN DE LA PRÁCTICA 2

Desde la ventana principal del ClarkConnect nos dirigimos a *Red > Outgoing.* A continuación escogemos el modo de tráfico (Block all outgoing traffic) y actualizamos:

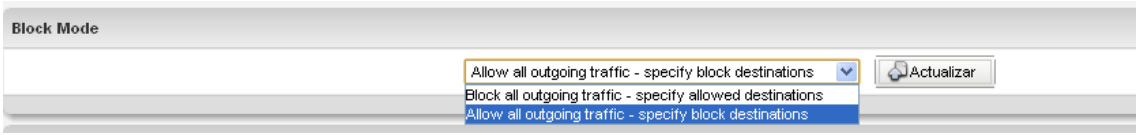


Fig. 87. Selección modo de bloqueo

Para esta práctica bloquearemos todo el tráfico de salida a excepción de los dominios **www.unitecnologica.edu.co** y **www.utbvirtual.edu.co** solo se podrá navegar solo en los dominios antes mencionado como se muestra a continuación:

Fig. 88. Dominios bloqueados

3.2.4. PRUEBA PRÁCTICA 2

Al momento de realizar la prueba se puede observar que el explorador web solo carga los dominios habilitados.

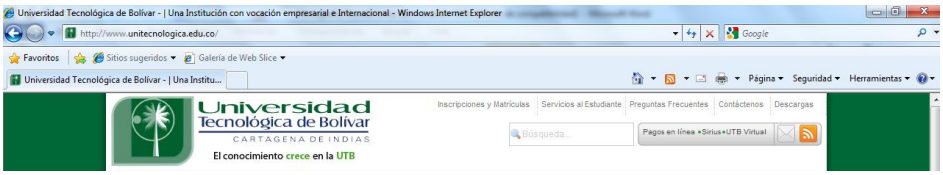


Fig. 89 Dominio www.unitecnologica.edu.co habilitado

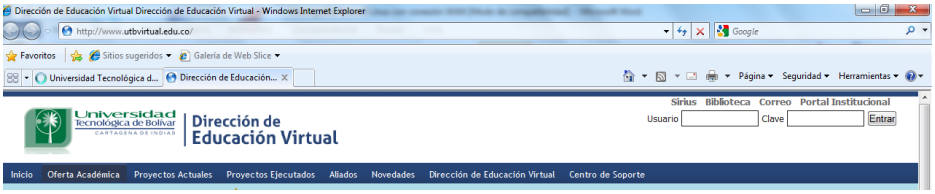


Fig. 90 Dominio www.utbvirtual.edu.co habilitado

3.3. PRÁCTICA 3: FILTRO DE PROTOCOLOS CLARKCONNECT

Antes de realizar la práctica debemos conocer cómo se conecta ClarkConnect a la Internet, las direcciones IP usadas y el DNS (**ver sección 2.2.3. y 2.2.5.**). Es necesario conocer este paso, así se tendrá mejor conocimiento de cómo bloquear un domino.

3.3.1. DESCRIPCIÓN DE LA PRÁCTICA

Esta práctica nos permitirá manejar lo que puede y no puede acceder el usuario en la red.

3.3.2. REQUERIMIENTOS

Para la ejecución de esta práctica se necesitan los siguientes módulos:

- *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, entre otros.

- *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.

3.3.3. ELABORACIÓN DE LA PRÁCTICA 3

Desde la ventana principal del ClarkConnect nos dirigimos a *Red* > Protocol Filter. Para esta ocasión bloquearemos protocolos de streaming audio para no permitir escuchar mp3 o música en forma streaming[22]. Procedemos a activar los diferentes filtros de contenidos como se muestra a continuación:

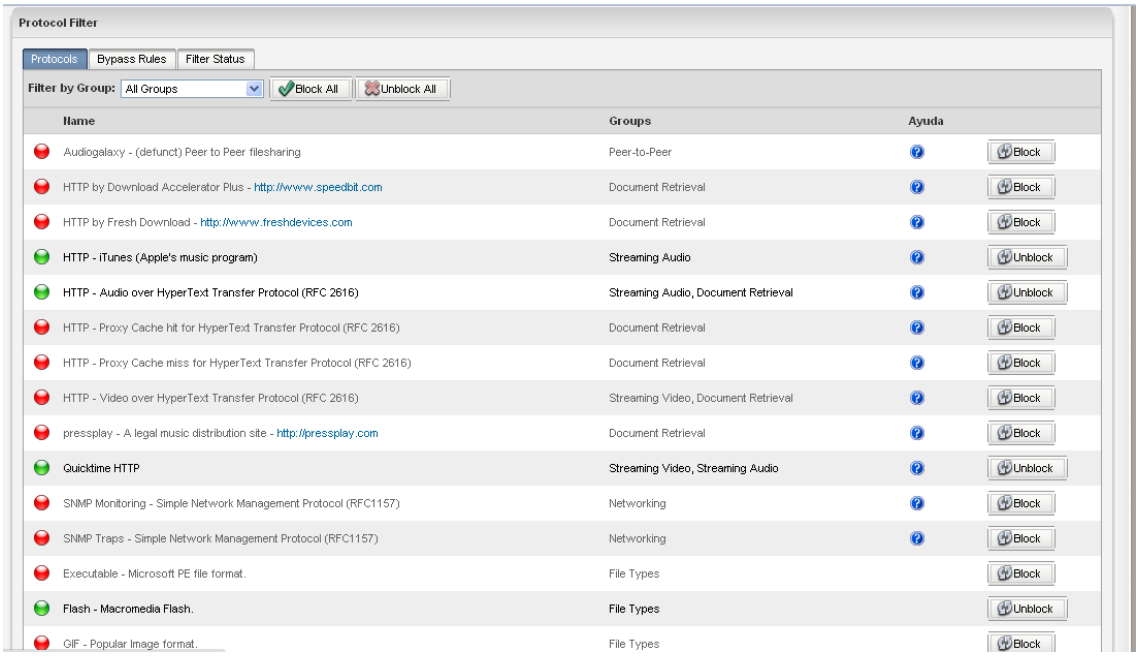


Fig. 91. Lista para filtrado por protocolo

[22] Consiste en la distribución de audio o video por Internet.

3.3.4. PRUEBA PRACTICA 3

Al momento de carga una página web que tenga contenido MP3 se puede ver como se bloquea los paquetes streaming de MP3 no se cargan.

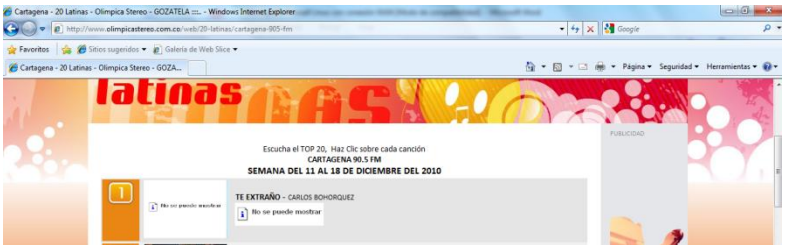


Fig. 92. Carga restringida de streaming MP3 del dominio

3.4. PRACTICA 4: BLOQUEANDO WINDOWS LIVE MESSENGER CLARKCONNECT

Antes de realizar la práctica debemos conocer cómo se conecta ClarkConnect a la Internet, las direcciones IP usadas y el DNS (**ver sección 2.2.3. y 2.2.5.**). Es necesario conocer este paso, así se tendrá mejor conocimiento de cómo bloquear un domino.

3.4.1. DESCRIPCIÓN DE LA PRÁCTICA

Se mostrara la forma de fácil y sencilla manera de bloquear una herramienta tan popular como lo es Windows Live Messenger

3.4.2. REQUERIMIENTOS

Para la ejecución de esta práctica se necesitan los siguientes módulos:

- *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, entre otros.
- *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.

3.4.3. ELABORACIÓN DE LA PRÁCTICA 4

Desde la ventana principal del ClarkConnect nos dirigimos a *Red* > Protocol Filter, Para esta ocasión bloquearemos filtrar grupo por Instant Messaging/chat y le aparece esta imagen a continuación:

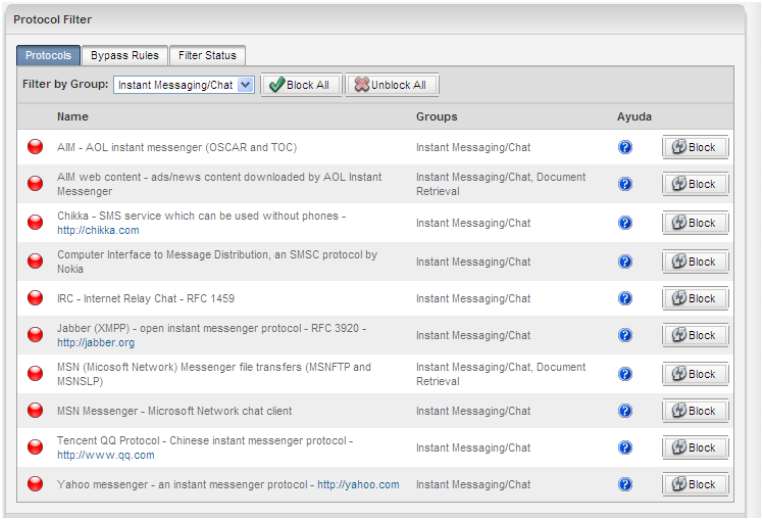


Fig. 93. Filtrada búsqueda MSN

Luego presionan *Block* en MSN Messenger y les aparece de color verde habilitado el bloqueo como muestra la imagen:

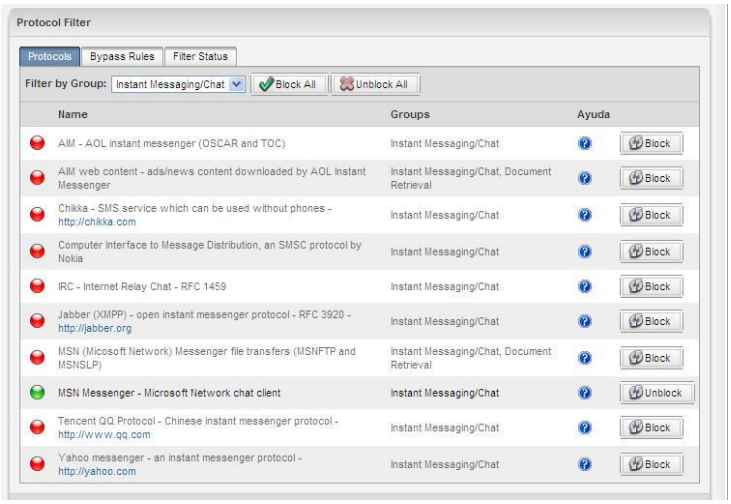


Fig. 94. Bloqueo MSN

3.4.4. PRUEBA PRACTICA 4

Al momento de realizar la práctica notamos en la imagen que la aplicación Windows Live Messenger no inicia sesión por que el servicio ha sido bloqueado.

Fig. 95. Acceso restringido a Windows Live Messenger

3.5. PRACTICA 5: BLOQUEANDO WEB DESDE FIRESTARTER

Antes de realizar la práctica debemos conocer cómo se conecta Firestarter a la Internet por medio de la distribución de Linux Kubuntu, las direcciones IP usadas y el DNS (**ver sección 2.3.1. y 2.3.4.**) Es necesario conocer este paso, así se tendrá mejor conocimiento de cómo bloquear un domino y/o IP

3.5.1. DESCRIPCIÓN DE LA PRÁCTICA

Esta práctica Permite que todo el tráfico de salida, a excepción del dominio bloqueado.

3.5.2. REQUERIMIENTOS

Para esta práctica se debe tener instalado y configurado la distribución de Linux Kubuntu 10.04 LTS y la aplicación Firestarter (ver sección 2.3 y anexo 1).

3.5.3. ELABORACIÓN DE LA PRACTICA 5

Desde la ventana principal del Firestarter nos dirigimos a la pestaña *Normativa.* Nos dirigimos al campo *Denegar conexiones al host* Para esta ocasión bloquearemos la web http://www.eluniversal.com.co/.

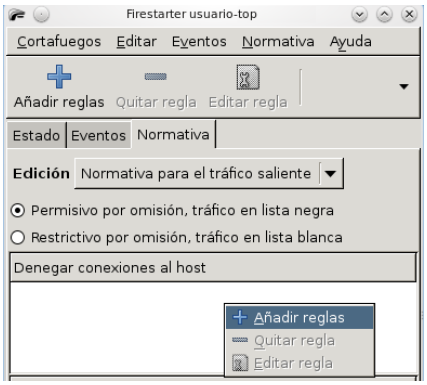


Fig. 96. Añadiendo reglas trafico saliente del Firestarter

Hacemos clic derecho en el campo *Denegar conexiones al host* y añadimos una nueva regla

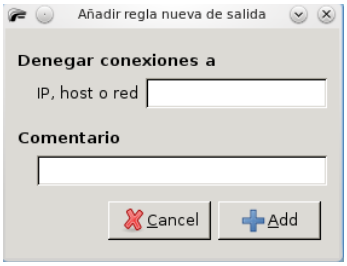


Fig. 97. Añadiendo nueva reglas trafico saliente del Firestarter

En esta ventana se añade la regla, ya sea para una dirección IP o para el dominio de la web que se desea bloquear en este caso la web del periódico El Universal.

3.5.4. PRUEBA PRACTICA 5

Al momento de realizar la práctica podemos notar que el dominio www.eluniversal.com.co no carga correctamente.

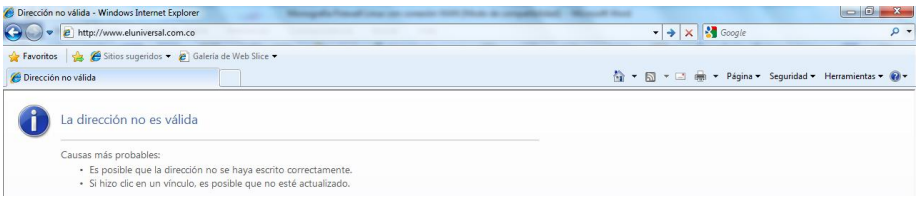


Fig. 98. No carga el dominio www.eluniversal.edu.co

CONCLUSIONES

Al finalizar el estudio, análisis y desarrollo de esta monografía pudimos notar que la implementación de un Firewall proporcionara herramientas para complementar la seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red y hacia la red externa.

Como resultado del proceso de implementación de firewall logramos reafirmar el objetivo de conocer los firewalls en su entorno cognoscitivo y aplicativo, en esta investigación nos basamos principalmente en el firewalls de filtrado de paquetes a nivel de la capa de Red.

Cabe descartar que la implementación de esta investigación del servidor Firewall se llevó acabo en un computador con el hardware necesario para instalar el Servidor/Firewall GNU/Linux, y se documentó todo el proceso al igual que la posterior configuración del servidor una vez instalado y se implementación en una red LAN.

Se realizaron prueba satisfactoria como filtrar de contenido web, paquete entre otros que pueden servir a un administrador de red pueda realizar de manera satisfactoria un servidor/firewall en la red telemática que vaya a realizar.

ClarkConnect y Firestarter son dos herramientas muy útiles para implementar firewalls en entornos de redes, pues nos permiten de manera muy sencilla, rápida y eficaz, implementar filtros de contenido, levantar servicios y crear reglas de restricción a dominios y limitar ancho de banda.

RECOMENDACIONES

Durante el desarrollo de esta investigación se debe tener claro los conceptos y características de los firewalls al momento de ser implementando utilizando el criterio de evaluación por el administrador de seguridad de redes en una organización, definiendo el tipo de firewall que debe ejecutar, luego del diseño de la topología de red y la tabla de enrutamiento para el servidor Firewall se permite tener claro los componentes que se interconectarán.

Este documento está dirigido a empresas, instituciones, organizaciones, estudiantes que estén relacionados con el tema de seguridad y redes de computadoras al igual que administradores de redes que deseen proteger una red con herramientas que explicamos detalladamente en este documento para el público expuesto.

Con esta investigación un administrador de redes puede implementar diferentes normativas que desee aplicar en las distintas interfaces que este configure previamente, para los servidores o estaciones que tenga en su empresa, además puede aumentar el ancho de banda del Internet de la empresa con la herramienta ClarkConnect con la solución Multi-WAN, en donde puede conectar dos o más conexiones a Internet a su sistema. La solución no sólo aumenta el ancho de banda disponible, sino que también proporciona failover automático de la red.

GLOSARIO

Adaptador o Tarjeta de Red: es el dispositivo que conecta físicamente el ordenador con una red.

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.

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): 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 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.

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 más importantes de un computador, allí se almacena físicamente la información electrónica con la cual trabaja el software, por ejemplo: un documento o un programa.

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 (cualquiernombre, hotmail), y así hasta varios niveles.

Firewall: es un dispositivo que funciona entre dos o más 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". 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.

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.

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.

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 sí 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 local. Es usado por procesos y programas para comunicarse entre sí por medio de protocolos de red. Puede ser usado también 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 ®.

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 porque es posible acceder a cualquier ubicación de ella aleatoria y rápidamente.

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.

P*2P (peer to peer)*: red donde usuarios de Internet (y/o servidores) se conectan entre sí a través de programas y protocolos como Ares o eMule para compartir archivos tales como: música, vídeos, imágenes, programas y documentos. Están 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 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") 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. 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 un 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 híper vínculo.

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 electrónico en Internet.

Software: conjunto de órdenes 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.

TCP (Transmision 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.
TCP/IP: protocolo para la comunicación fiable de datos en una de red, es uno de los protocolos más 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". El TCP/IP es la base bajo la cual el Internet está construido.

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, \\PC1.

4. BIBLIOGRAFÍA

ARROYO, José. Linux Máxima Seguridad edición especial. México D.F. Editorial. Prentice Hall 2000.

DIAZ, José Manuel. Academia de Networking de Cisco Systems: fundamentos de seguridad de redes, especialista en Firewall Cisco, Madrid: Cisco Systems, 2005.

PICOUTO Fernando, LORENTE Iñaki, GARCIA Jean Paul, Ramos Antonio. Hacking y Seguridad en Internet. México D.F. Edit. Alfaomega Grupo Editor 2008.

[Libro en línea] DEAL, Richard A. Técnicas Cisco Router Firewall Security. http://books.google.com.co/books?id=vTfFNrkm5YcC&printsec=frontcover&dq=firewall&hl=es&ei=dQYETZeIGIyt8AaNmf3qAg&sa=X&oi=book_result&ct=result&resnum=10&ved=0CFYQ6AEwCQ#v=onepage&q&f=false

[Sitio Web] Point Clark Networks. Página oficial ClarkConnect.
Link: http://www.ClarkConnect.com/legacy/index.php

[Sitio Web] JUNNONEN, Tomas. Página oficial Firestarter - Documentación.
Link: http://www.fs-security.com/docs.php

[Sitio Web] Página oficial GNU – Documentación.
Link: http://www.GNU.org/doc/doc.html

[Sitio Web] Página oficial Kubuntu – Documentación.
Link: https://wiki.kubuntu.org/Kubuntu/GettingInvolved/Documentation

[Articulo Web] FERRUSOLA, Víctor. Beneficios de un Firewall en Internet
Link: http://lanrouter.com/index.php?option=com_content&task=view&id=38&Itemid=71

[Articulo Web] Diccionario online
Link: http://www.lawebdelprogramador.com/diccionario/#

ANEXOS

ANEXO 1. INSTALACION Y CONFIGURACION DE GNU/ LINUX KUBUNTU 10.04 LTS

¿QUÉ ES KUBUNTU?[23]

Kubuntu es una distribución GNU/Linux derivada de Ubuntu, que usa el entorno de escritorio KDE (el cual es más configurable) en lugar del GNOME que usa Ubuntu. En general, la mayoría de las cosas se hacen de la misma manera que en Ubuntu, pero difiere en algunos aspectos relacionados con el entorno gráfico. Todos los paquetes comparten los mismos archivos que Ubuntu. Todos los paquetes comparten los mismos archivos que Ubuntu.

PASOS A SEGUIR PARA LA INSTALACIÓN DE KUBUNTU 10.04 GNU/LINUX Y LA APLICACIÓN DE FIREWALL FIRESTARTER

Qué se necesita para poder instalar un GNU/Linux Kubuntu 10.04:

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.
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 Kubuntu 10.04.
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.

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 firewall con el S.O. Kubuntu 10.04 y Firestarter necesita obligatoriamente 2 tarjetas de red para su funcionamiento.

[23] http://www.guia-ubuntu.org/index.php?title=Gu%C3%ADa_Kubuntu

HARDWARE BASE	
Procesador / CPU	Hasta cuatro procesadores - Pentium®, Celeron®, AMD Athlon®
Memoria RAM	Como mínimo se recomienda 512 MB
Disco Duro	Como mínimo se recomienda 1 GB de almacenamiento
Unidad Óptica / CD-ROM	Requerido
Tarjeta de video	Cualquier tarjeta de video
Tarjeta de Sonido	Opcional
PERIFÉRICOS	
Mouse	Requerido
Monitor y Teclado	Requerido
RED	
Conexión a Internet (Broadband)	Ethernet, banda ancha , DSL o conexión wireless
Tarjetas (adaptadoras de red)	PCI, ISA o PCMCIA Wireless

Tabla 3. Requerimientos para la instalación SO Kubuntu 10.04 GNU/LINUX

INSTALACIÓN KUBUNTU 10.04 GNU/LINUX EN EL SERVIDOR FIREWALL

La instalación de Kubuntu habitualmente suele tomar unos 30 minutos si no hay ningún problema. Pasos a seguir:

Primero deberemos descargar el CD de instalación de Kubuntu 10.04. El archivo descargado será una imagen ISO que deberemos grabar en un disco para proceder con la instalación. Todos los programas de grabación de discos son capaces de hacer esto (Ej.: Nero Burning, Alcohol 120%, Daemon entre otros).

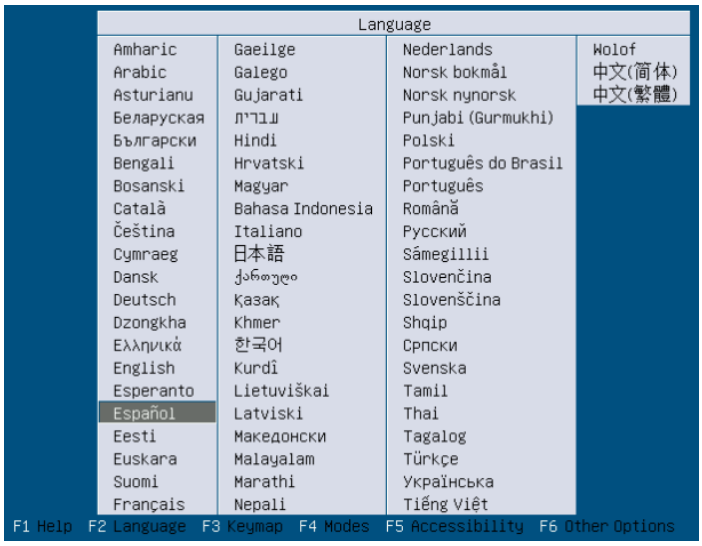


Fig. 99. Configuración lenguaje SO Kubuntu 10.04 GNU/LINUX

Después de encender el servidor e introducir el CD de instalación aparecerá la pantalla de bienvenida. Aquí nos pide escoger el idioma de configuración e instalación de Kubuntu. [F1] Ayuda, [F2] Idiomas, [F3] Teclado, [F4] Modos, [F5] Accesibilidad, [F6] Otras opciones. En nuestro caso nos interesa instalar y configurar en español, así que escogemos y presionamos [*Enter*].

Fig. 100. Bienvenida SO Kubuntu 10.04 GNU/LINUX

Cuando termine nos mostrara una serie de opciones, en este caso nos interesa la opción 2 la cual es instalar el S.O.

No tenemos que hacer más que esperar a que cargue y comience el asistente de instalación (installation wizard).

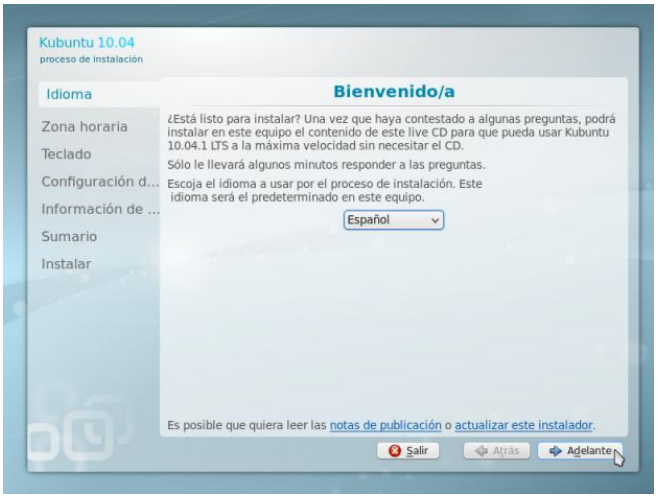


Fig. 101. Configuración Idioma SO Kubuntu 10.04 GNU/LINUX

Elegir el idioma. Si en la pantalla de bienvenida eligió el español, simplemente pulse adelante («Siguiente» o «Adelante»), en otro caso seleccione «Español» en la lista, y continúe.

Fig. 102. Configuración zona horaria SO Kubuntu 10.04 GNU/LINUX

Elegir la zona horaria. Simplemente pulse sobre su zona para acercar el mapa y después sobre la ciudad concreta representativa de su huso horario. Por ejemplo, en este caso se escogió región *Colombia* y zona horaria *Hora de Colombia.*

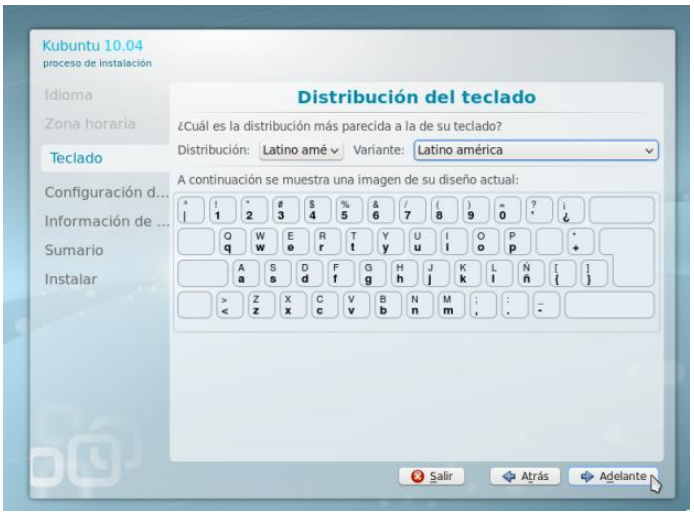


Fig. 103. Configuración zona horaria SO Kubuntu 10.04 GNU/LINUX

Elegir el tipo de teclado. Si todo va bien y no tiene un teclado fuera de lo común sino un teclado español estándar, debería estar ya seleccionado (teclado «Latino América»). Cerciórese de que esto es así escribiendo en la caja de texto que hay en la parte inferior, pulsando algunas teclas específicas del español, como la «ñ» y algunos símbolos habituales como el peso «$».

Fig. 104. Configuración disco duro SO Kubuntu 10.04 GNU/LINUX

Nota: Este es uno de los pasos más importantes y delicados. Se trata de indicar dónde se debe instalar Kubuntu*. Escoja la opción correcta o podría formatear una partición no deseada si va a compartir el disco duro con otros sistemas operativos.*

Existen tres opciones:

1. *Borrar y usar el disco entero:* Elija ésta si desea borrarlo todo y usar el disco duro por defecto como único para Kubuntu. Es la opción más fácil y menos problemática. Se utilizó esta opción para este instructivo.
2. *Especificar particiones manualmente (avanzado)*: Con esta opción, podrá especificar cómo serán las particiones de forma más específica. Ésta no es la mejor opción si nunca se ha hecho una partición o se ha instalado GNU/Linux antes.

De cualquier modo, aconsejable utilizar la opción 1 si no se tiene conocimiento de cómo particionar el disco duro.

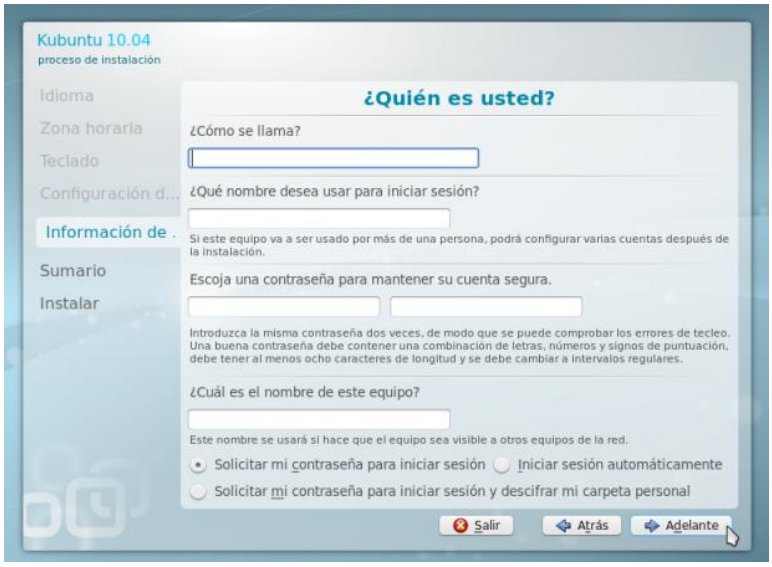


Fig. 105. Configuración información de usuario SO Kubuntu 10.04 GNU/LINUX

En este paso de la instalación le preguntará sus datos: su nombre real y su nombre o apodo de usuario. Por ejemplo, el nombre real podría ser «wilmer padilla» y el nombre de usuario «jmiranda». A continuación, escoja una contraseña y el nombre del ordenador. Puede dejar el que se asigna por defecto, por ejemplo «miranda-laptop» o «padilla-desktop».

¡Evitar olvidar la contraseña, ya que sin ella nos quedamos sin poder acceder al sistema operativo! Se recomienda colocar contraseña con números, caracteres especiales, letras mayúsculas y minúsculas. Mínimo 14 caracteres.

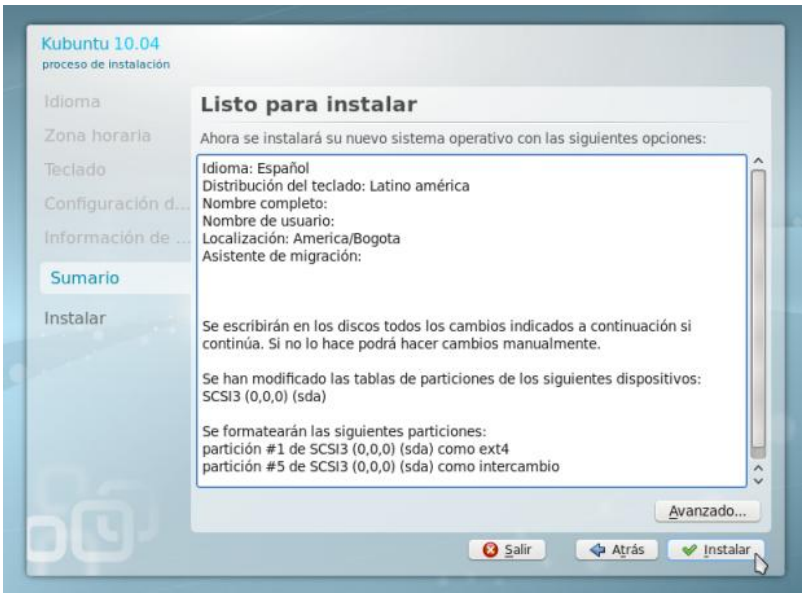


Fig. 106. Sumario SO Kubuntu 10.04 GNU/LINUX

En la pantalla siguiente, el instalador le mostrará los datos para que los revise. Asegúrese de que todo está en orden y pulse «Siguiente» para comenzar a copiar los archivos de Kubuntu al disco duro.

¡Felicitaciones! Acabamos de finalizar la etapa de configuración para la instalación. Si durante el proceso de instalación tenemos conexión a Internet, el programa de instalación se conectará y descargará los paquetes necesarios para dejar nuestra instalación de Kubuntu completamente en nuestro idioma.

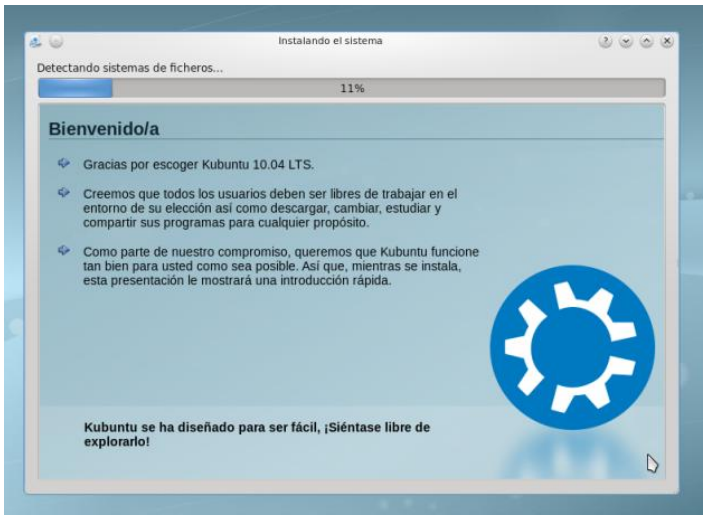


Fig. 107. Instalación SO Kubuntu 10.04 GNU/LINUX

En la siguiente pantalla se detectan y se crean los sistemas de ficheros con los cuales trabajara nuestro S.O. Kubuntu 10.04.

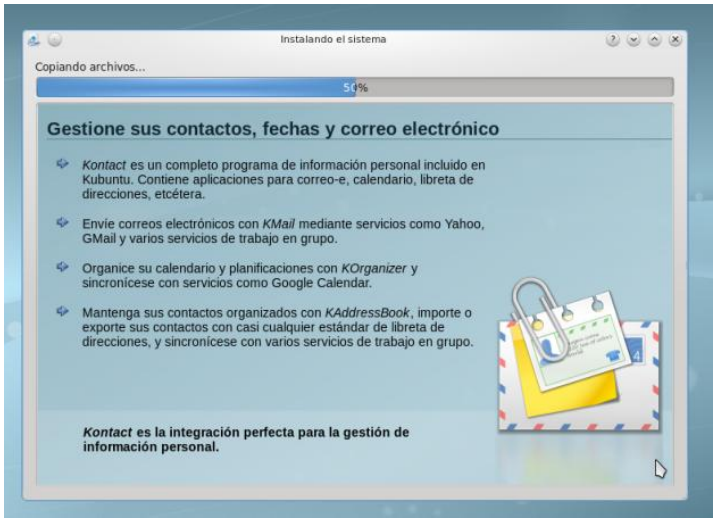


Fig. 108. Copia de archivos SO Kubuntu 10.04 GNU/LINUX

Sólo basta esperar mientras se instala y carga todos los archivos necesarios para el terminar con la instalación del sistema.

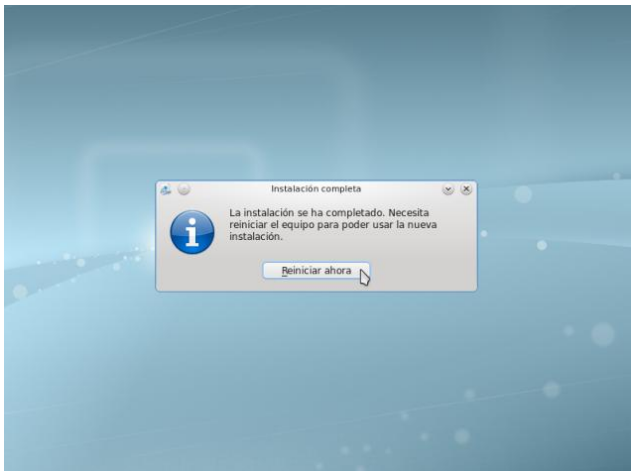


Fig. 109. Finalización de instalación SO Kubuntu 10.04 GNU/LINUX

Si todo se instaló correctamente, al final la instalación le preguntará si desea reiniciar (sin el disco) y nos solicitará reiniciar el sistema para completar la instalación.

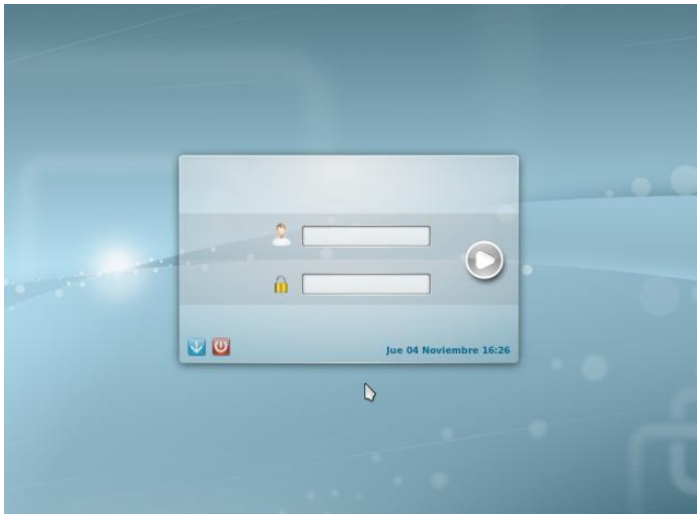


Fig. 110. Autenticación Sesión del SO

Después de haber reiniciado el servidor nos pedirá retirar cualquier disco o CD de la unidad. El sistema operativo nos pedirá el usuario y contraseña colocado durante la configuración de instalación.