UNIVERSIDAD DEL AZUAY

FACULTAD DE ADMINISTRACION

ESCUELA DE INGENIERIA DE SISTEMAS

FIREWALLS Y SEGURIDAD EN INTERNET MEDIANTE IPCop

Trabajo de graduación previo a la obtención del título de

INGENIERO DE SISTEMAS

AUTORES: CESAR CABRERA V.
PAOLA NARVAEZ C.

DIRECTOR: ING. HERNAN GAVILANES

CUENCA, ECUADOR

2006

DEDICATORIA

Queremos dedicar este trabajo a nuestros padres por el esfuerzo y apoyo incondicional que siempre nos han brindado. Por ser pieza fundamental en nuestro desarrollo personal.

AGRADECIMIENTOS

Nuestro principal agradecimiento es para Dios por permitirnos realizar este trabajo y a nuestros profesores quienes han sido los que nos han permitido llegar hasta este punto de nuestra carrera en especial para los Ingenieros Pablo Esquivel y Hernán Gavilanes quienes nos han brindado su apoyo y sus conocimientos para poder realizar este trabajo.

INDICE DE CONTENIDOS

RESUMEN

Actualmente el constante manejo de información por medio de Internet y el intercambio de datos entre ordenadores es de uso habitual para en empresas u oficinas lo que ha generado un incremento de riesgos a los que puede estar sometido su ordenador y la información que maneja, por lo que es necesario tener un sistema que brinde seguridad monitoreada es decir, proteger los equipos y proveer el acceso seguro a Internet.

Hacer uso de una aplicación firewall permite controlar el tráfico de información en Internet utilizando varias interfaces de red además brindar la seguridad necesaria en nuestro lugar de trabajo.

El proyecto IPCop es un proyecto que ofrece un firewall con características de distribución independiente que lo convierten en una herramienta útil para todo tipo de usuarios, independientemente de su nivel técnico. Se pretende brindar un buen nivel de seguridad a través de la aplicación IPCop.

El proyecto comprenderá:

- Análisis completo de un Firewall así como de la aplicación a utilizar.
- Implementación de la aplicación IPCop.
- Manejo de la información

_____

Ing. Hernán Gavilanes
DIRECTOR DE MONOGRAFIA

ABSTRACT

At the moment the constant handling of information by means of Internet and the exchange of data among computers is of habitual use in companies or offices what has generated an increment of risks to those that it can be subjected its computer and the information that it manages, for what is necessary to have a system that offers monitored security that is to say, to protect the computers and to provide the sure access to Internet.

To make use of a firewall application allows to control the traffic of information in Internet using several net interfaces, also to offer the necessary security in our work place.

The project IPCop is a project that offers a firewall with characteristic of independent distribution that converts it in a useful tool for all type of users, independently of its technical level. It is sought to offer a good level of security through the application IPCop

The project will understand:

- Complete analysis of a Firewall as well as of application to use.
- Implementation of the application IPCop.
- Manage of the information

INTRODUCCION

La seguridad es una característica de cualquier sistema ya sea informático o no, que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro.

Actualmente el constante manejo de información e intercambio de datos entre ordenadores mediante Internet y otras aplicaciones genera un incremento de riesgos a los cuales puede estar sometido uno o mas ordenadores, lo que nos motiva a buscar una manera de seguridad ante la posibilidad de que ocurra un ataque o suceda algún problema durante el intercambio de información.

IPCop permitirá mantener al margen a los usuarios no-autorizados (tales, como: hackers, crakers, vándalos, y espías) fuera de la red y proporcionar la protección para varios tipos de ataques posibles, asegurando el activo más importante que es la información. Ratificando así nuestro objetivo de instalar y configurar la aplicación de un firewall para imponer una política de seguridad en una o varias PC’s interconectadas en red.

CAPITULO I

INTRODUCCION

Existen diferentes maneras de proteger la información cuando una organización desea conectar su red privada a Internet., sin embargo, el uso de firewalls nos ayuda a aplicar restricciones al tráfico entrante, sin tomar en cuenta el tipo de negocios, se ha incrementado el numero de usuarios de redes privadas por la demanda del acceso a los servicios de Internet. Los administradores de red tienen que aumentar la seguridad de sus sistemas, debido a que se expone la estructura privada de sus datos así como la infraestructura de su red a los Expertos de Internet (Crakers).

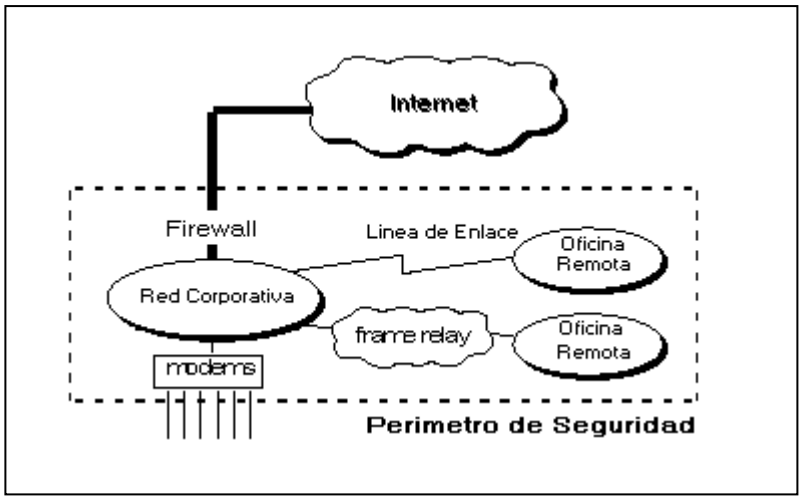
Para brindar el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Aún, si una organización no esta conectada al Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

FIREWALL

Un **cortafuegos** o **firewall**, es un elemento de hardware o software utilizado en una red de computadoras para prevenir algunos tipos de comunicaciones prohibidos según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red. La idea principal de un cortafuego es crear un punto de control de la entrada y salida de tráfico de una red. Un cortafuego correctamente configurado es un sistema adecuado para añadir protección a una instalación informática.

Un Firewall impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cuales de los servicios de red pueden ser accesados dentro de ésta, por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desgraciadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

FIGURA 1. 1 ESQUEMA DE UN FIREWALL



Beneficios de un Firewall:

- Administrar los accesos posibles del Internet a la red privada.
- Evita el ataque de otros servidores en el Internet.
- Permite al administrador de la red definir un "choke point" (embudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red.
- Prohibir potencialmente la entrada o salida de archivos sospechosos en la red
- Proporciona protección para varios tipos de ataques posibles.
- Simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran la red privada.
- Ofrecer un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, generar una prevención ante el riesgo de que ocurra un ataque, o suceda algún problema en el manejo de la información.
- Monitorea y registra el uso de Servicios de WWW y FTP, Internet.

Políticas de un Firewall:

El sistema firewall describe la filosofía fundamental de la seguridad en la organización, se debe tomar en cuenta estas dos políticas:

- "No todo lo específicamente permitido esta prohibido"

  Un firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso. Es recomendada únicamente a un limitado número de servicios soportados cuidadosamente seleccionados en un servidor.

La desventaja es que el punto de vista de "seguridad" es más importante que - facilitar el uso - de los servicios y estas limitantes numeran las opciones disponibles para los usuarios de la comunidad.

- "Ni todo lo específicamente prohibido esta permitido"

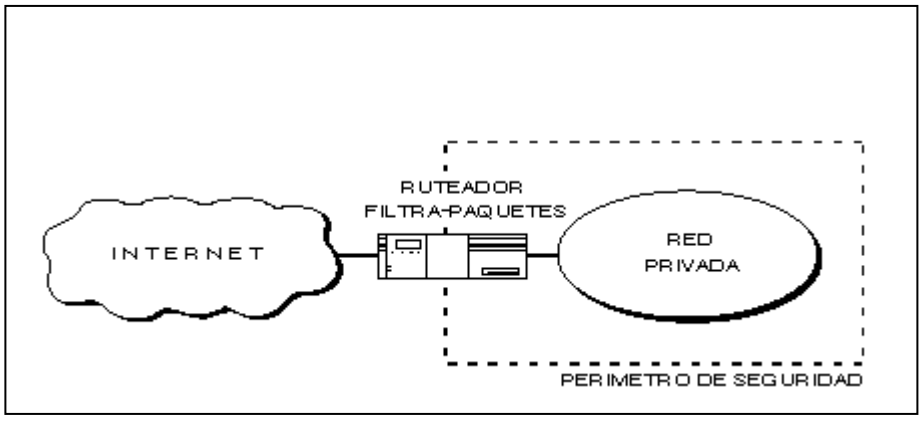
  Un firewall puede trasladar todo el tráfico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso. Esto crea ambientes más flexibles al disponer más servicios para los usuarios de la comunidad. La desventaja de esta postura se basa en la importancia de "facilitar el uso" que la propia - seguridad - del sistema. También además, el administrador de la red esta en su lugar de incrementar la seguridad en el sistema conforme crece la red. Desigual a la primer propuesta, esta postura esta basada en la generalidad de conocer las causas acerca de los que no tienen la habilidad para conocerlas

Si no se cuenta con la información detallada de la política a seguir, aun que sea un firewall cuidadosamente desarrollado, estará exponiendo la red privada a un posible atentado.

Componentes de un Sistema Firewall:

1. Ruteador Filtra-paquetes: Toma las decisiones de admitir/permitir el paso de cada uno de los paquetes que son recibidos.

FIGURA 1. 2 ESQUEMA DE UN RUTEADOR DE PAQUETES



Las características típicas de filtrado que un administrador de redes podría solicitar en un ruteador filtra-paquetes para perfeccionar su funcionamiento serian:

- Permitir la entrada de sesiones Telnet únicamente a una lista especifica de servidores internos.
- Permitir la entrada de sesiones FTP únicamente a los servidores internos especificados.
- Permitir todas las salidas para sesiones Telnet.
- Permitir todas las salidas para sesiones FTP.
- Rehusar todo el trafico UDP.

A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. Se permiten filtrados según campos de nivel de transporte como el puerto origen y destino, o a nivel de enlace de datos como la dirección MAC

2. Gateway a Nivel-aplicación. Permiten al administrador de red la implementación de una política de seguridad estricta. El Gateway a nivel-aplicación deja que la información circule entre los sistemas pero no permite el intercambio directo de paquetes. El principal riesgo de permitir que los paquetes se intercambien dentro y fuera del sistema se debe a que el servidor residente en los sistemas de protección de la red podrá ser asegurado contra cualquier amenaza representada por los servicios permitidos.

Es descrito como un "servidor de defensa" porque es un sistema diseñado específicamente blindado y protegido contra cualquier ataque, posee las siguientes características:

- La plataforma de Hardware del servidor de defensa ejecuta una versión "segura" de su sistema operativo.
- Únicamente los servicios que el administrador de redes considera esenciales son instalados

El Gateway a nivel-aplicación da a la administración de red un completo control de cada servicio desde aplicaciones Proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede acceder a los servicios. Tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información detallada de registro. Los filtrados se pueden adaptar a características propias de los protocolos de este nivel.

3. Gateway a Nivel-circuito: Es 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.

   Se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un Gateway "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida. Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización de los ataques externos.

CONCLUSIONES

Los riesgos de seguridad a los que está sometida una red son múltiples, unos provienen directamente de accesos al sistema y otros de las conexiones que se realizan. Además se debe tener en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables. Es por esto que vemos la necesidad de la existencia de un firewall para la aplicación de barreras y procedimientos que resguardan el acceso a los datos para personas autorizadas.

Sin embargo, cabe recalcar que un cortafuegos correctamente configurado es un sistema adecuado para añadir protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

CAPITULO II

INTRODUCCION

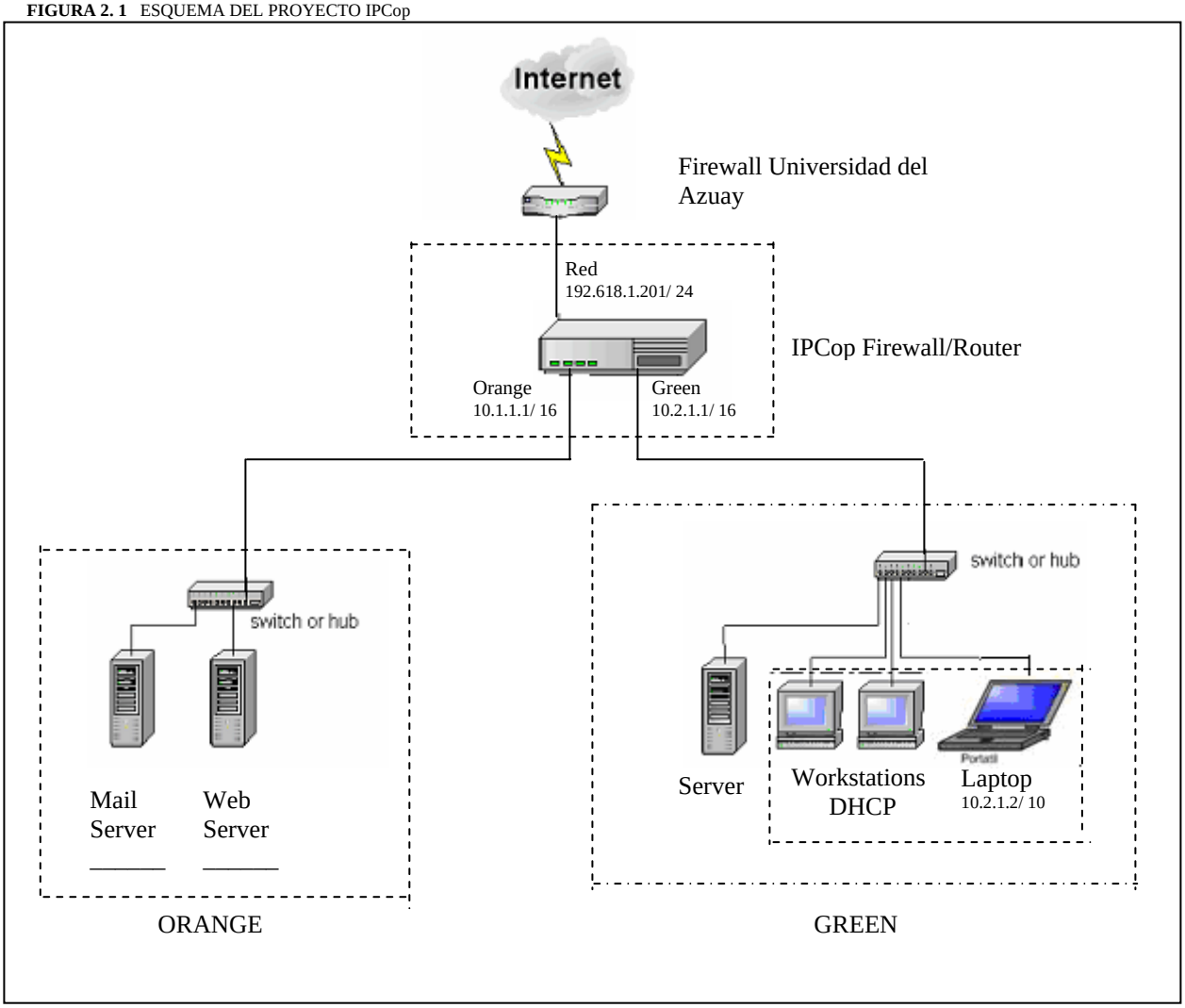
Los firewalls están sufriendo una enorme conversión como resultado de la constante evolución de amenazas. Es por esto que el proyecto IPCop nos sirve de ayuda, ya que ofrece un firewall de buenas características en forma de una distribución independiente. Además de esto para instalar IPCop no necesitamos de un hardware muy potente lo que beneficia al usuario para tener mayor seguridad en la transferencia de datos a bajo costo.

IPCop es una Distribución de Linux especializada; completa y preparada para proteger su red, es distribuido bajo la Licencia de General de GNU. Este creció fuera de muchas necesidades. La primera de esas necesidades era una protección segura de nuestras redes personales y comerciales, ofrece un firewall con características de distribución independiente que lo convierten en una herramienta útil para todo tipo de usuarios, independientemente de su nivel técnico.

Se pretende brindar servicios de configuración, acceso a Internet y Proxy a una red de área local LAN garantizando un buen nivel de seguridad y controlar el tráfico de información.

APLICACIÓN DE UN FIREWALL

FIGURA 2. 1 ESQUEMA DEL PROYECTO IPCop



Para la instalación de IPCop utilizaremos el siguiente hardware

- Una máquina con un procesador AMD Athlon(tm) XP 2000 y 512MB de RAM, 20GB de disco duro y 3 tarjetas de red
- 1 switch 3Com10/100/1000 de 16 puertos
- Cables de red
- CD grabado con la imagen ISO de IPCop

IPCop utiliza un sistema de codificación basado en colores (rojo, verde, azul y naranja) para describir los papeles o niveles de seguridad que los interfaces/segmentos tendrán en la protección de nuestra red.

Código de colores utilizado por IPCop

El código de colores es lógico y representa un entorno continuo de acceso a la red. Estructurado de la siguiente manera:

FIGURA 2. 2 CODIGO DE COLORES PROYECTO IPCop

COLOR	DETALLE
Rojo	Prohibido
Verde	Confianza Total
Azul	Integración de Servicios wireless
Naranja	Implementación de segmento DMZ es decir el lugar donde se sitúan los servidores que tendrán acceso al público como Internet

El orden de fidelidad de redes en el orden de confianza creciente es:

$$\text{RED} \longrightarrow \text{ORANGE} \longrightarrow \text{BLUE} \longrightarrow \text{GREEN}$$

En nuestro proyecto vamos a hacer una instalación de red verde/rojo/naranja con 3 interfaces de red uno de los cuales conecta a un segmento diferente: Internet, DMZ y red local.

INSTALACIÓN DE IPCOP

Cuando se instala IPCop en un PC, la unidad de disco duro se estructurará y se perderán todos los datos en él.

Hay tres posibles maneras de instalar IPCop que podemos ver en la siguiente tabla:

FIGURA 2. 3 METODOS PARA LA INSTALACION DE IPCop

Table 1.2. Media required for different installation methods

Method	Boot Floppy	Driver Floppy	CD Drive	FTP/Web Server
Bootable CD	N	N	Y	N
Bootable Floppy with CD	Y	N	Y	N
Bootable Floppy with FTP/Web Server	Y	Y	N	Y

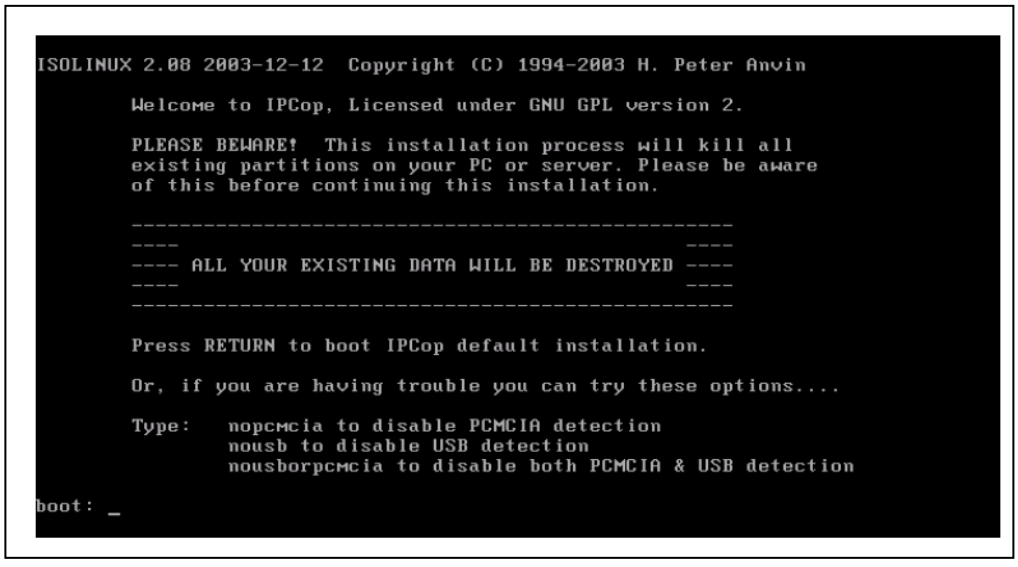
Proceso de instalación

Conectamos todos los elementos físicos (cables de red, etc…).

Como primera instancia necesitamos tener disponible monitor, teclado y ratón sobre la máquina en la que instalaremos IPCop

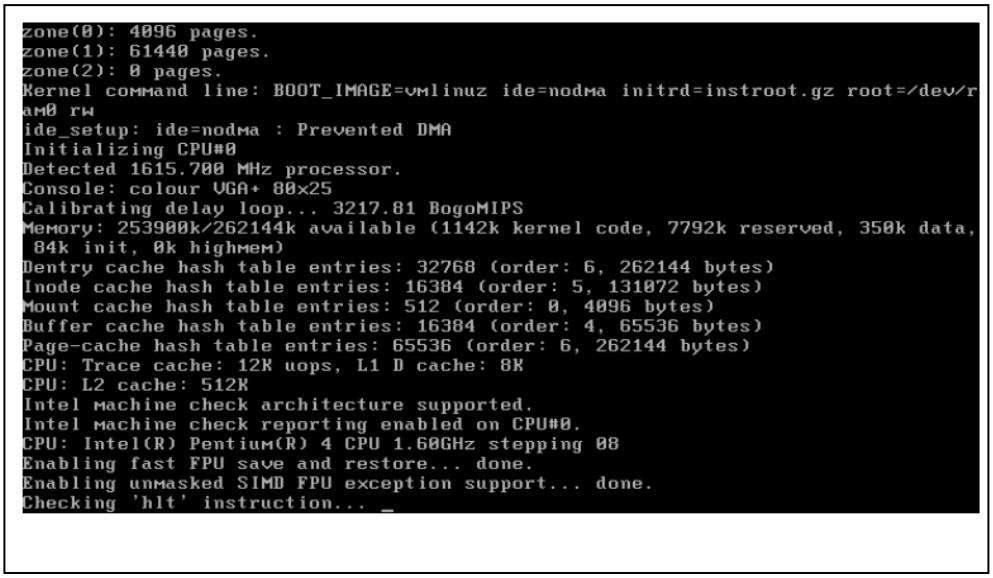
1. Arrancaremos desde el CD y visualizamos una pantalla que contiene una advertencia que todos sus datos existentes se destruirán

FIGURA 2. 4 PROCESO DE INSTALACION PANTALLA Nro. 1



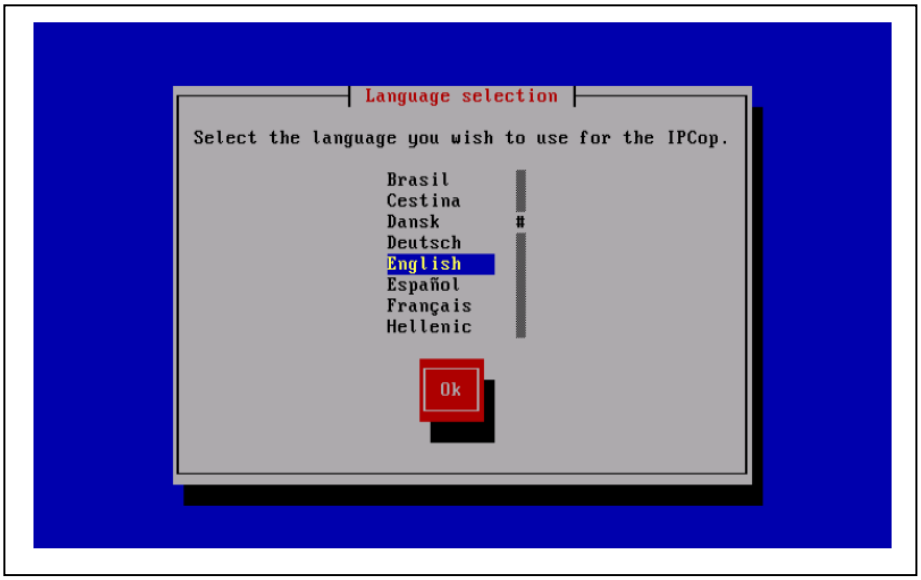
A continuación aparecerán varios mensajes informativos que pueden ignorarse a menos que sea un problema del hardware

FIGURA 2. 5 PROCESO DE INSTALACION PANTALLA Nro. 2



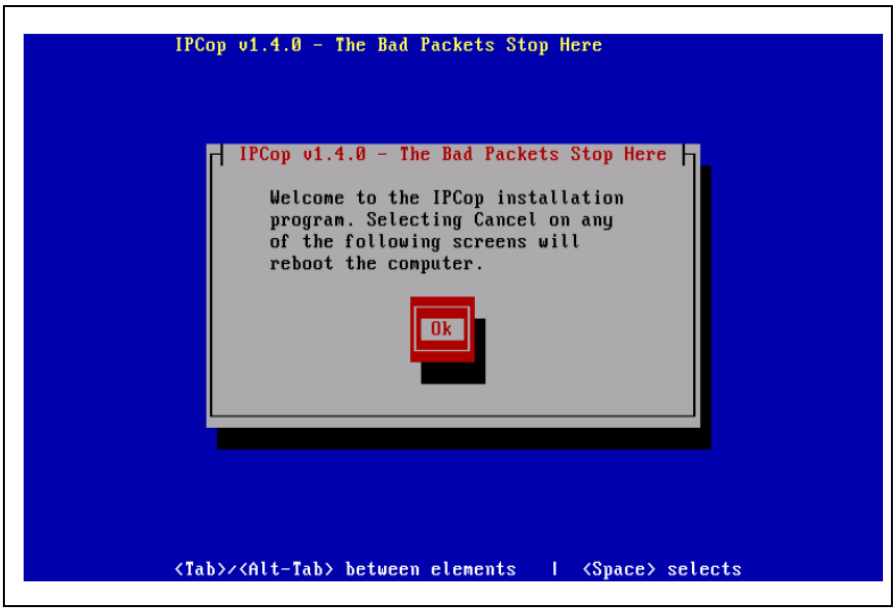
2. Elegir el idioma en la siguiente pantalla y desde aquí en adelante todos los cuadros de diálogos y menús de la instalación aparecerán en el idioma escogido

FIGURA 2. 6 PROCESO DE INSTALACION PANTALLA Nro. 3



3. La siguiente pantalla simplemente nos indica como cancelar la instalación en caso de ser necesario

FIGURA 2. 7 PROCESO DE INSTALACION PANTALLA Nro. 4

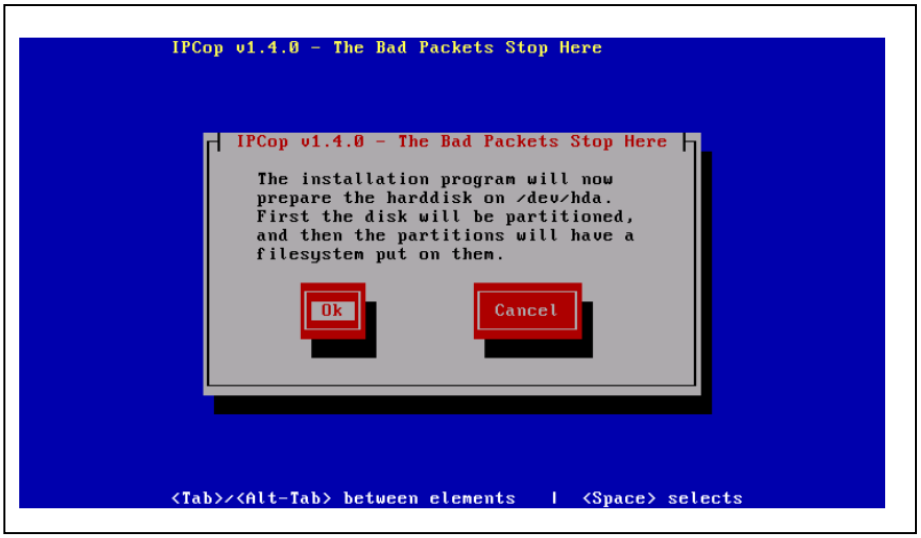


4. El próximo cuadro de diálogo nos permite elegir la fuente de instalación, en nuestro caso un CD.

FIGURA 2. 8 PROCESO DE INSTALACION PANTALLA Nro. 5

5. Aparece la última advertencia acerca del particionamiento del disco.

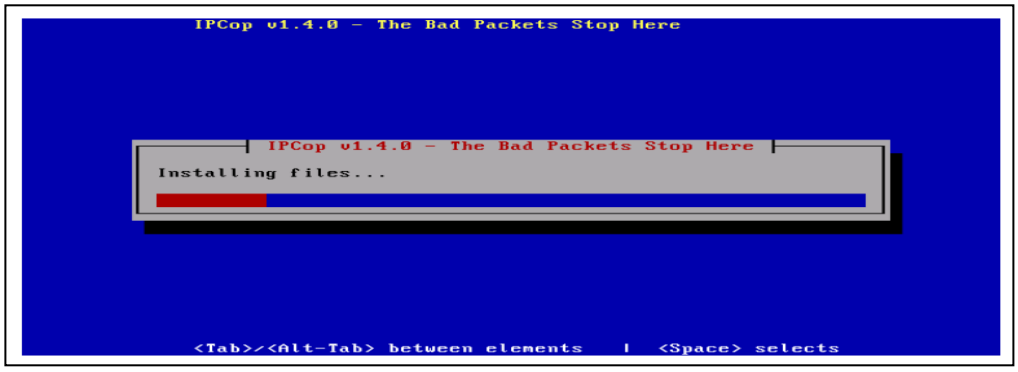
FIGURA 2. 9 PROCESO DE INSTALACION PANTALLA Nro. 6



Después de que usted selecciona que Ok y Enter en esta pantalla todos los datos en su unidad de disco duro se borrará

6. Luego IPCop estructurará y dividirá su unidad de disco duro. Entonces instalará todos sus archivos.

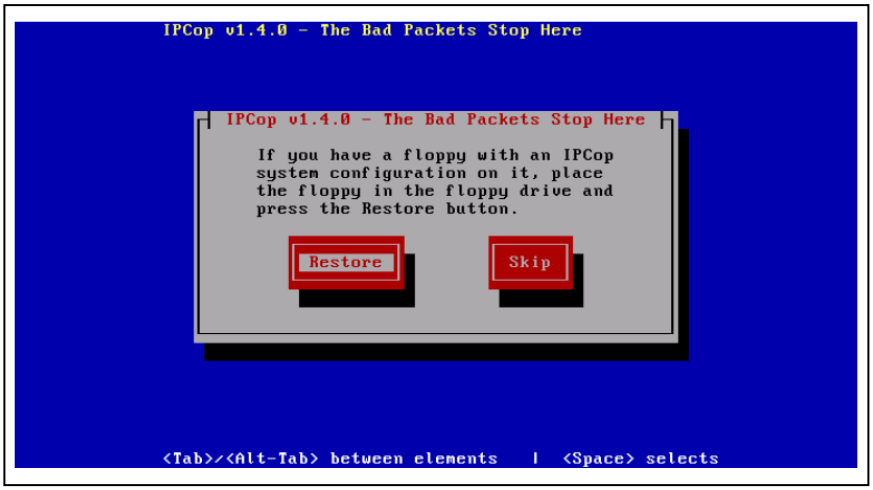
FIGURA 2. 10 PROCESO DE INSTALACION PANTALLA Nro. 7



7. Usted tiene la opción de restaurar los archivos de un IPCop es decir hacer una copia de seguridad. Para esto selección Restore e introduzca los disquetes en la

unidad y luego Enter. Por otra parte, si desea ignorarlo presione Skip y luego Enter.

FIGURA 2. 11 PROCESO DE INSTALACION PANTALLA Nro. 8

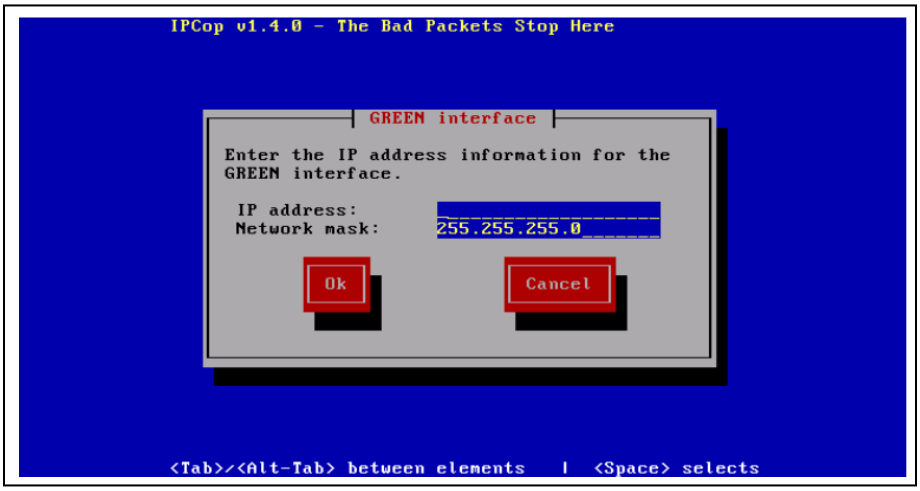


8. Luego IPCop permite configurar las tarjetas de red. El método más rápido de configurar nuestros interfaces de red es elegir la opción **Probe**. Si se conoce la información exacta de tus tarjetas de red podemos elegirlas desde la opción **Select**.

FIGURA 2. 12 PROCESO DE INSTALACION PANTALLA Nro. 9

9. La siguiente pantalla a continuación, requiere que introduzcamos una dirección de red para el interfaz verde (**Green Interface**). Introducimos la dirección en el campo **IP Address** y 255.255.255.0 en el campo **Network mask**.

FIGURA 2. 13 PROCESO DE INSTALACION PANTALLA Nro. 10



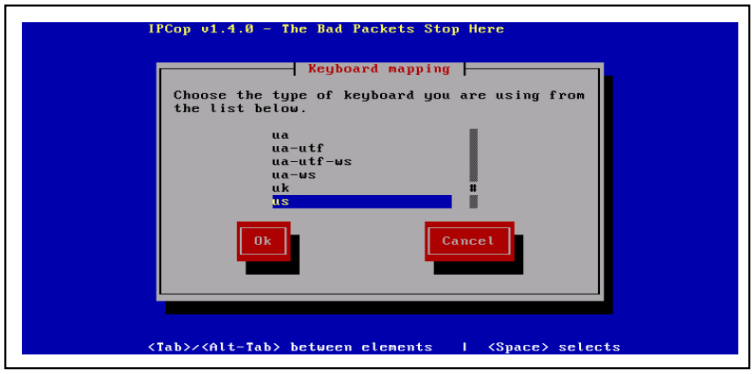
10. A continuación IPCop formatea y se instala en el disco duro. Una vez terminada la instalación se pide que reiniciar la máquina y al arrancar nos ejecutará la utilidad **Setup** mediante la cual se llevará a cabo la configuración inicial del sistema

FIGURA 2. 14 PROCESO DE INSTALACION PANTALLA Nro. 11

La Configuración Inicial

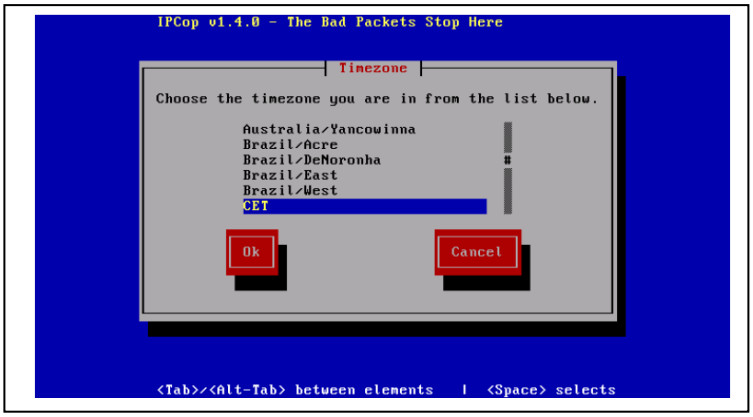
1. La primera pantalla le permite configurar su teclado.

FIGURA 2. 15 PROCESO DE INSTALACION PANTALLA Nro. 12



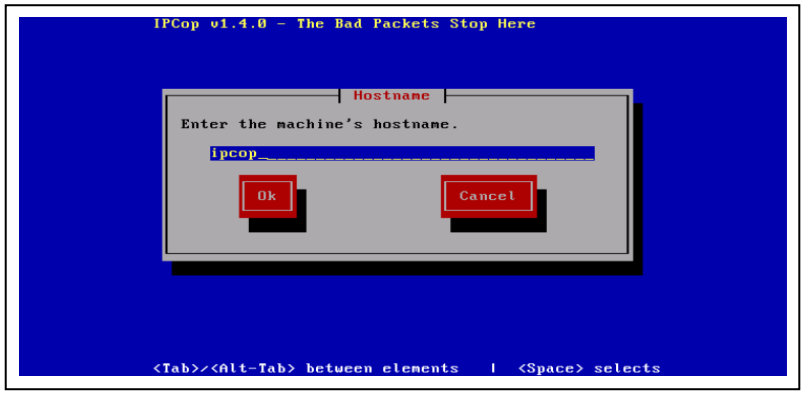
2. La siguiente pantalla, nos pide la zona horaria.

FIGURA 2. 16 PROCESO DE INSTALACION PANTALLA Nro. 13



3. Luego debemos configurar el hostname de su máquina.

FIGURA 2. 17 PROCESO DE INSTALACION PANTALLA Nro. 14



4. Se debe configurar el nombre del dominio de su máquina de IPCop.

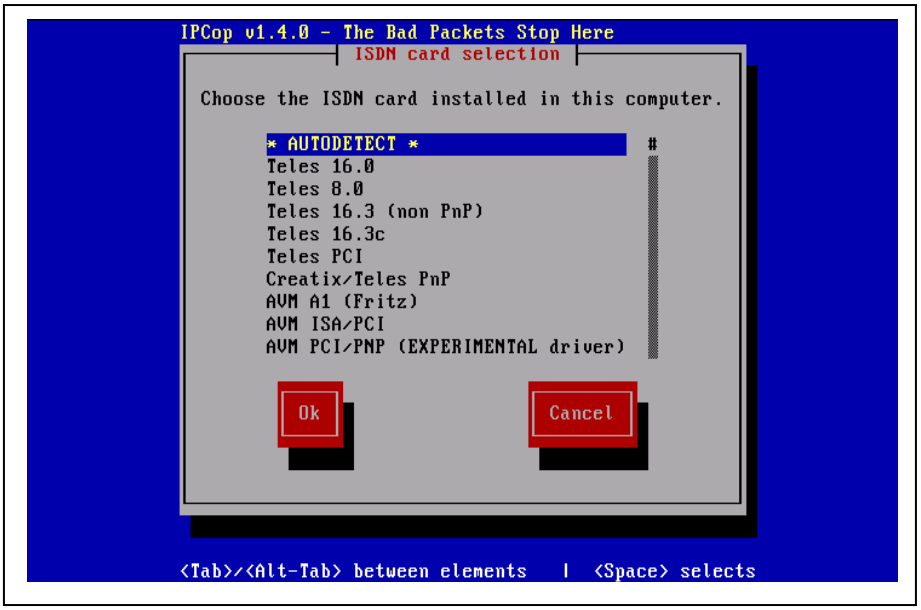
FIGURA 2. 18 PROCESO DE INSTALACION PANTALLA Nro. 15

5. La siguiente pantalla nos permite configurar el ISDN.

FIGURA 2. 19 PROCESO DE INSTALACION PANTALLA Nro. 16

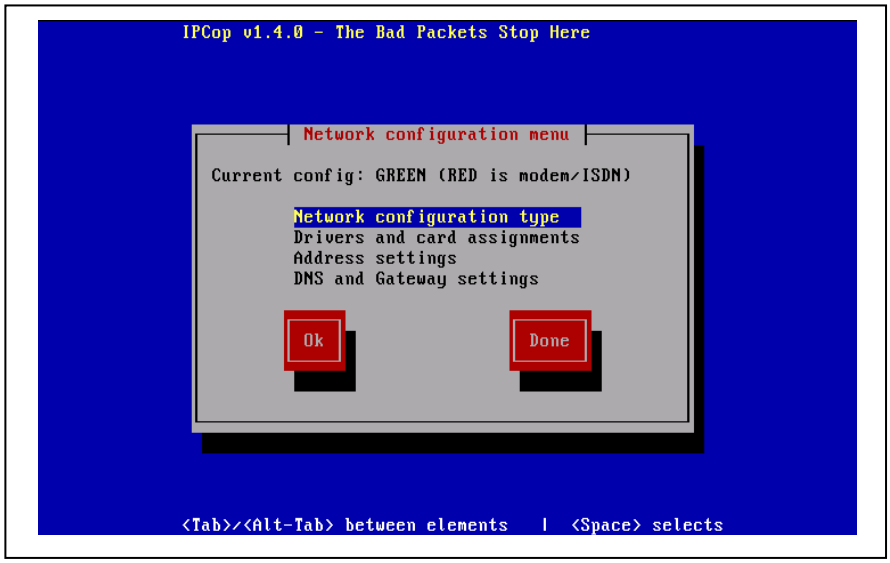
6. Luego se debe poner parámetros de los drivers para su tarjeta, en este caso seleccionamos la opción AUTODETEC para que IPCop la identifique automáticamente.

FIGURA 2. 20 PROCESO DE INSTALACION PANTALLA Nro. 17



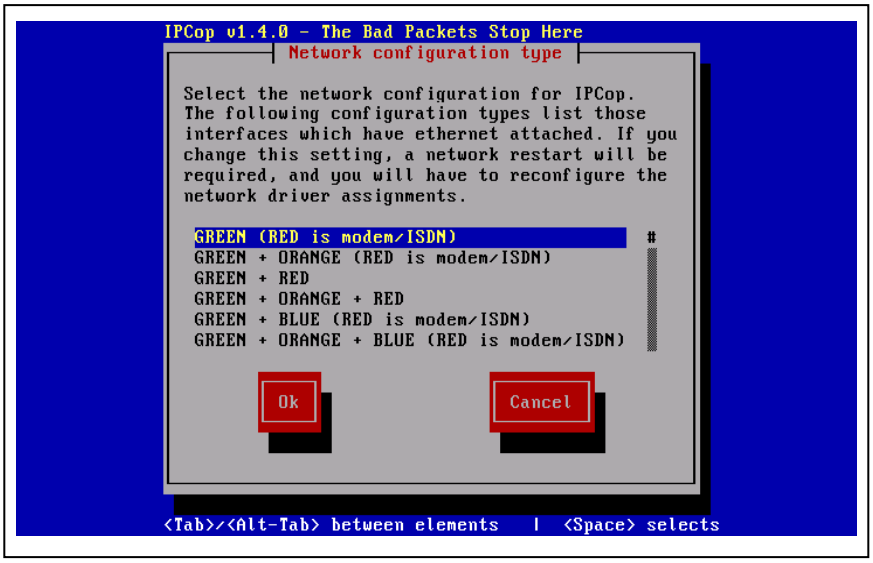
7. Se debe configurar las interfaces de la red siguiendo los pasos que nos proporciona el menú de configuración.

FIGURA 2. 21 PROCESO DE INSTALACION PANTALLA Nro. 18



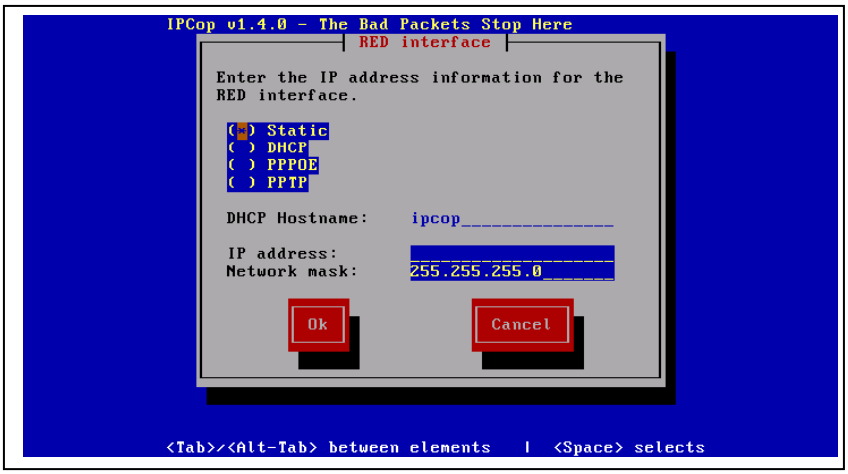
8. El Menú de Configuración de Red nos presenta cuatro interfaces de red: ROJA VERDE, AZUL y NARANJA. Este cuadro de diálogo nos permite escoger el tipo de configuración de red. En nuestro caso escogimos la opcion GREEN + ORANGE + RED

FIGURA 2. 22 PROCESO DE INSTALACION PANTALLA Nro. 19



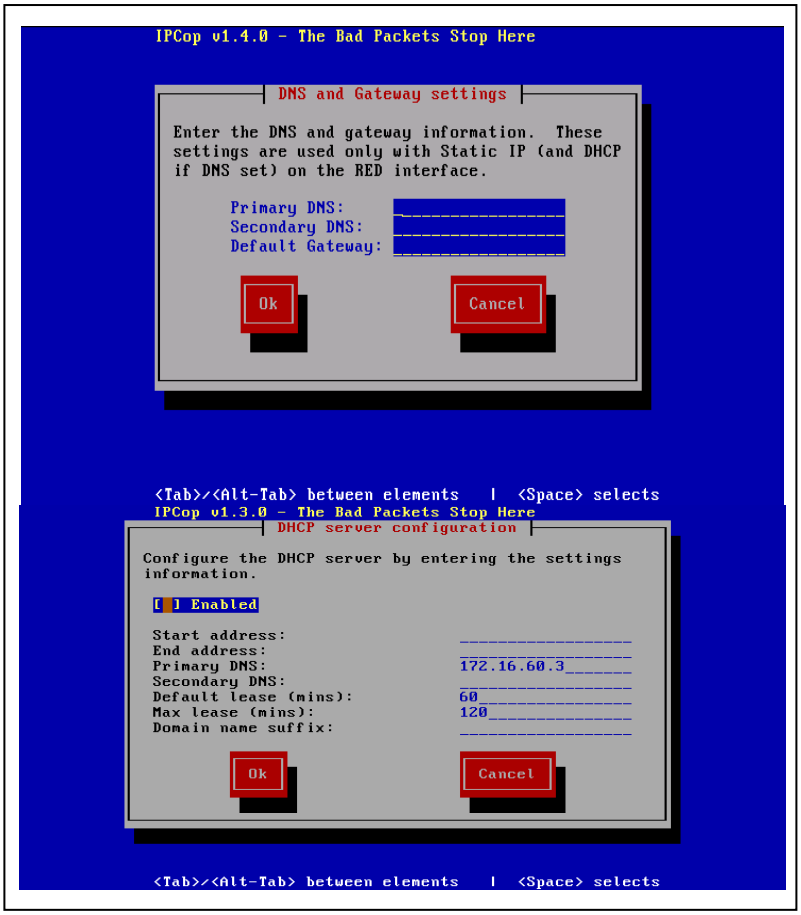
9. Cuando usted selecciona Ok, regresamos al Menú de Configuración de Red, Ahora debemos configurar las direcciones de red y el medio por el cual se obtendrá la dirección IP. Nuestra interfaz ROJA trabaja de forma estática con la dirección 192.168.1.201 y con máscara de red 255.255.255.0 para así poder conectarnos a la red pública de la Universidad del Azuay

FIGURA 2. 23 PROCESO DE INSTALACION PANTALLA Nro. 20



10. Luego se solicita la configuración del DNS del equipo y el DHCP Server, debemos ingresar los parámetros indispensables como DNS primario y secundario y el sufijo de DNS para configurar en las estaciones de trabajo de la red VERDE.

FIGURA 2. 24 PROCESO DE INSTALACION PANTALLA Nro. 22



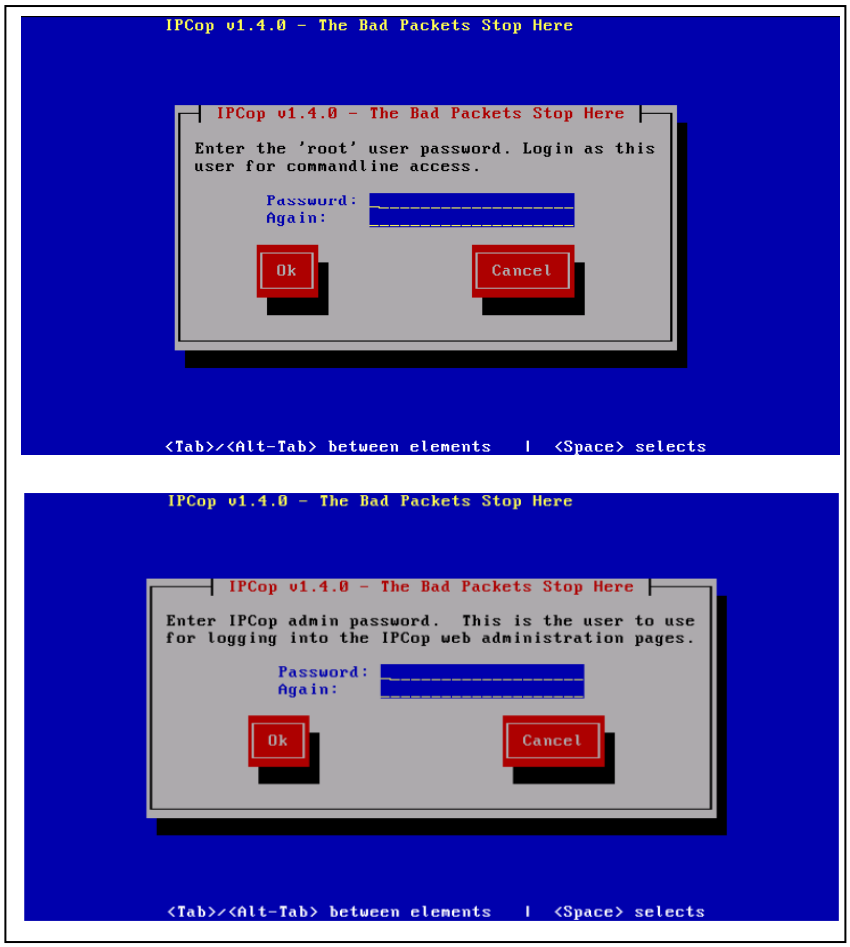
11. Ahora se nos solicita que se ingresen las passwords para los usuarios principales de la distribución, esta contraseña debe ser segura para no permitir el acceso a usuarios no autorizados o intrusos en la red.

    Esta distribución genera automáticamente 2 usuarios para realizar las diferentes tareas de administración:

    ROOT: Usuario utilizado para el acceso mediante la línea de comando.

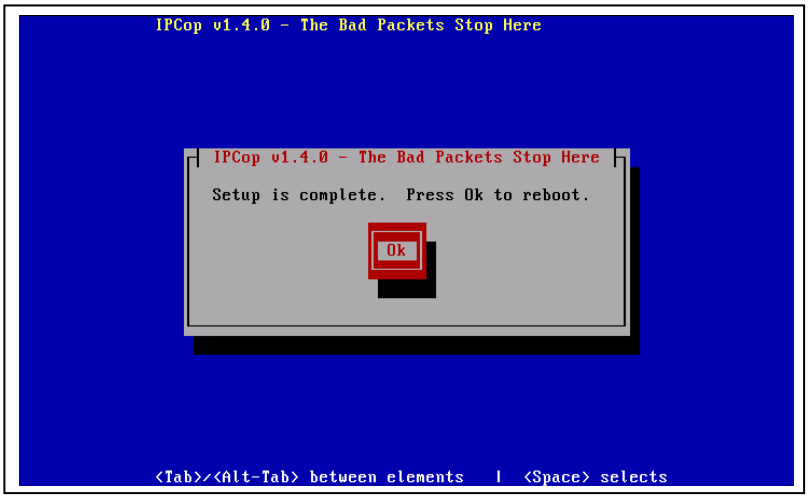
    ADMIN: Usuario para acceder vía HTTPS.

FIGURA 2. 25 PROCESO DE INSTALACION PANTALLA Nro. 23



12. Al finalizar la Configuración inicial de IPCop nos muestra la siguiente pantalla

FIGURA 2. 26 PROCESO DE INSTALACION PANTALLA Nro. 24



CONCLUSIONES

Podemos decir IPCop intenta imitar a los firewalls en su concepto como una aplicación que cumple la única función de ser firewall pudiendo administrarse casi en su totalidad de forma remota. Además es útil para brindar seguridad en una red ofreciendo los servicios de Proxy, DHCP lo que facilita a la que la red interna se convierta más vulnerable.

Se debe tomar en cuenta los diferentes pasos a seguir en la instalación ya que es una de las tecnologías mas recientes que hay en el filtrado de paquetes bajo linux implementada en las versiones de kernel superiores. Permite el filtrado de paquetes a través de reglas lo que permite un mayor control de las actividades del usuario

CAPITULO III

INTRODUCCION

IPCop nos permite crear *barreras y procedimientos* que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo. Antes de poner en marcha una aplicación es necesario realizar una serie de pruebas que nos ayudaran a corregir errores y crear nuevas estrategias. Además nos permite saber si su funcionamiento va de acuerdo con las exigencias de nuestra interfaz de red.

Las pruebas se realizaran de acuerdo a la guía de administración de IPCop la cual nos permite revisar la instalación y configuración de la aplicación, proporcionándonos las modelos a seguir para cada una de las funciones y servicios.

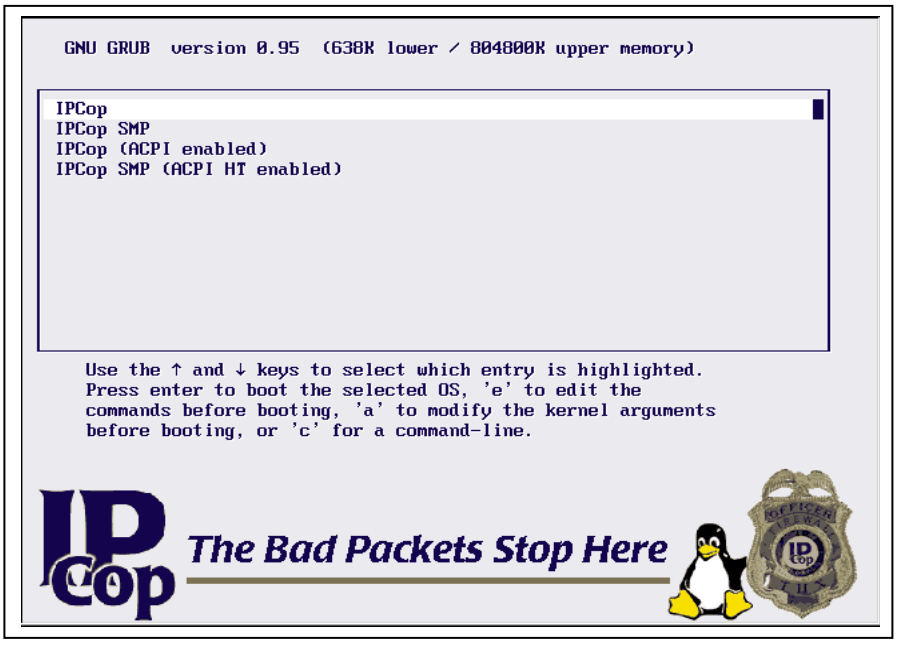
El principal objetivo de realizar estas pruebas es conseguir resultados efectivos que nos garanticen imponer una política de seguridad en una o varias PC's interconectadas en red, además mejorar seguridad mediante el uso de IPCop.

PRUEBAS

Revisión de la Instalación y Configuración

IPCop nos presenta la siguiente pantalla al momento de encender la máquina que tiene instalado el firewall.

FIGURA 3.1 PROCESO DE CONFIGURACION PANTALLA Nro. 1



Para la revisión de la instalación debemos asegurarnos que podamos acceder a IPCop vía web browser. Para acceder a IPCop GUI se debe ingresar la dirección IP de la interfaz de verde u hostname de su servidor de IPCop junto con director del puerto:

Puerto 81: http://10.2.1.1:81

Puerto 445 (puerto seguro): https://10.2.1.1:445

Entonces nos aparecerá la siguiente pantalla en donde nos permite:

Conectar: Permite forzar a una conexión a Internet

Desconectar: Permite terminar la conexión a Internet

Refrescar: Actualiza la información sobre la pantalla principal

FIGURA 3.2 PROCESO DE CONFIGURACION PANTALLA Nro. 2

La página de administración nos permite navegar entre 7 diferentes menús:

- SISTEMA
- ESTADO
- RED
- SERVICIOS
- FIREWALL
- VPN
- LOGS

Menú Sistema:

Este grupo de opciones se plantea para ayudarle a administrar y controla al servidor de servidor.

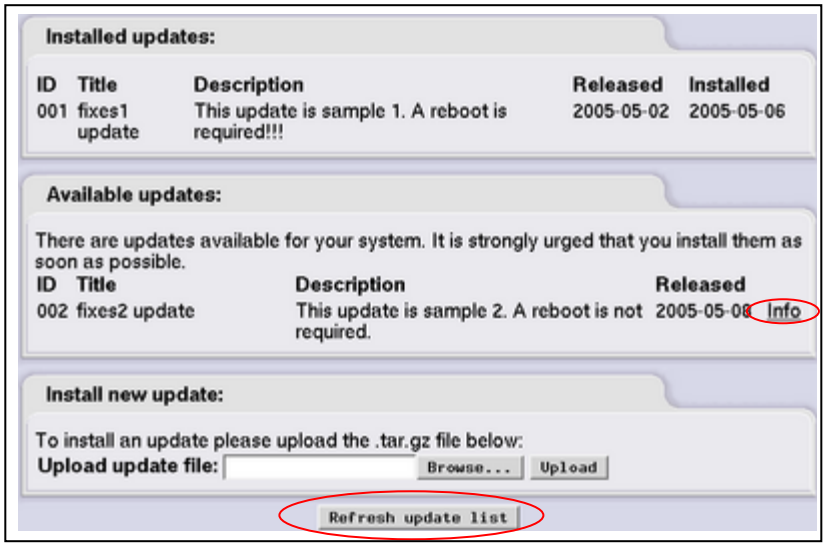
1. Actualizaciones AW

   Esta tiene 3 secciones la primera muestra su nivel del parche actual, la segunda lo informa de nuevos parches disponibles y la tercera le permite aplicar un nuevo parche. Cada vez que nos conectamos al Internet, IPCop verificará si existe una

nueva Actualización que puede estar disponible. También podemos verificar manualmente las actualizaciones haciendo clic el Refrescar la lista actual.

Cuando un nuevo parche está disponible se visualizara la información sobre la pantalla con una descripción corta y un link, para ver mas información damos clic en el link “Info” y aparecerá una pagina con la información completa.

FIGURA 3.3 PROCESO DE CONFIGURACION PANTALLA Nro. 3



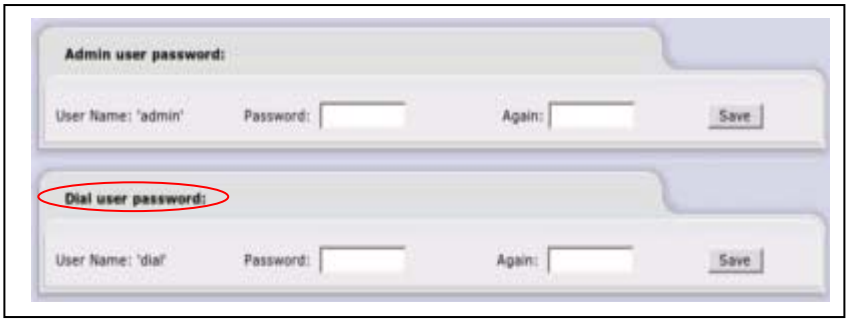
Se recomienda leer la información completa sobre el parche antes de aplicarlo al servidor de IPCop para evitar cualquier falla en el sistema.

2. Passwords

Esta opción nos permite cambiar el Admin y/o contraseñas de Usuario Dial, como usted requiera. Simplemente debemos ingresar la contraseña deseada en el campo para el Usuario, confirmamos nuevamente la contraseña y damos un clic en Guardar. Ingresando la contraseña del Dial se activa el Dial ID del usuario

Este usuario especial tiene la habilidad posee los suficientes permisos para usar los botones en la IPCop, pero no tiene la autoridad del admin en el cortafuego.

FIGURA 3.4 PROCESO DE CONFIGURACION PANTALLA Nro. 4



3. Accesos SSH

Esta opción le permite decidir si el acceso de SSH remoto está disponible en su servidor de IPCop o no. Para activar el acceso de SSH remoto activamos la casilla de verificación. También es posible configurar varios parámetros de SSH. La opción de SSH es por defecto inválida y nosotros aconsejaríamos que solamente se habilite cuando sea necesario.

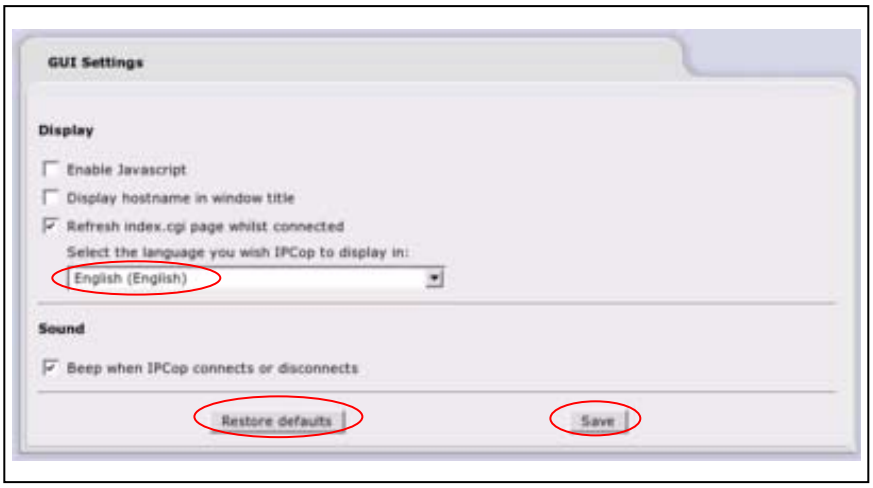
FIGURA 3.5 PROCESO DE CONFIGURACION PANTALLA Nro. 5

4. GUI Settings

En esta opción podemos controlar el lenguaje de IPCop y como funcionan y aparecen las páginas de IPCop. Después de realizar cualquier cambio, damos un

clic en el botón Guardar. Para restaurar los valores predeterminados damos un clic en el botón Restaurar Valores predeterminados, y luego Guardar.

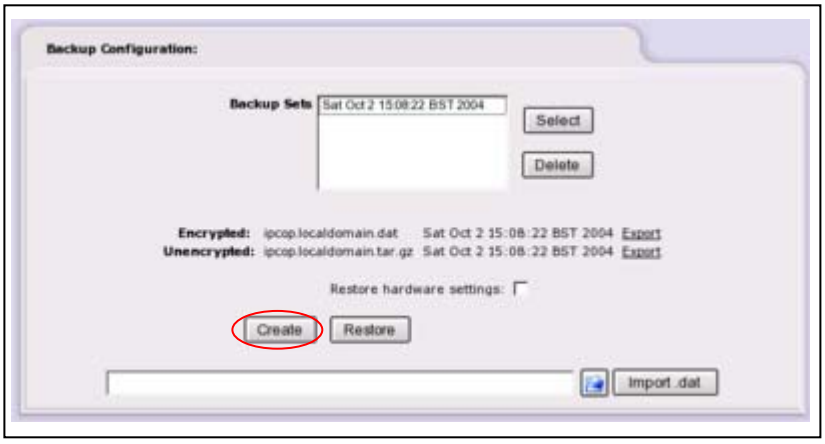
FIGURA 3.6 PROCESO DE CONFIGURACION PANTALLA Nro. 6



5. Respaldos de la Pagina WEB

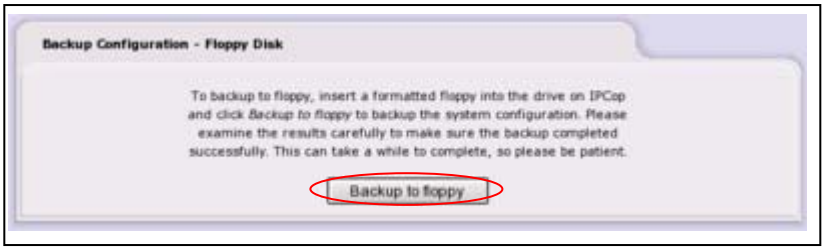
Esta opción nos permite crear respaldos, se crea un disco de respaldo lo que nos ayuda a ahorrar la cantidad de datos. En la siguiente pantalla podemos controlar la creación, exporte, importe y restauración de respaldos de archivos de IPCop. Haciendo clic en el botón Crear se crearan los archivos de respaldo.

FIGURA 3.7 PROCESO DE CONFIGURACION PANTALLA Nro. 6



También nos permite en la siguiente pantalla tener respaldo de la Configuración de IPCop en un disco flexible haciendo clic en el botón Respaldo con disco flexible.

FIGURA 3.8 PROCESO DE CONFIGURACION PANTALLA Nro. 7

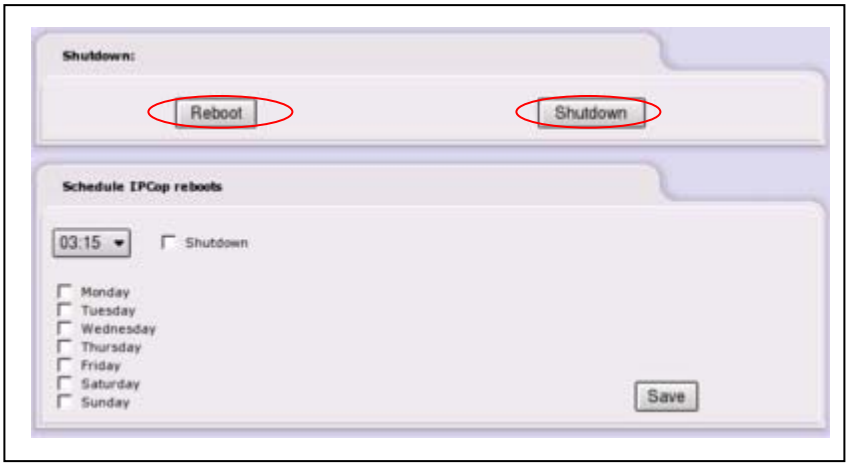


Todos los mensajes que aparecen durante la realización de un respaldo se guardaran en el campo Información.

6. Apagar el IPCop

Esta opcion permite Apagar o Reiniciar el sistema del servidor de IPCop. Simplemente damos pulse el botón el Shutdown o Reboot. Ademàs permite controlar y el día dando clic en el botón Guardar.

FIGURA 3.9 PROCESO DE CONFIGURACION PANTALLA Nro. 8



Menú Estado:

1. Estado del Sistema

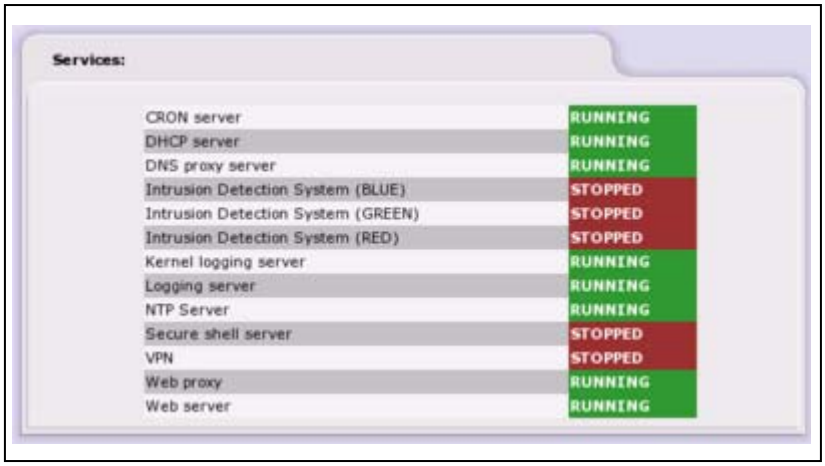
Esta opcion nos permite una completa información con respecto al

el estado actual de su servidor de IPCop. Consta de la siguiente subdivisión:

a) Servicios

Despliega los servicios que se están ejecutando actualmente.

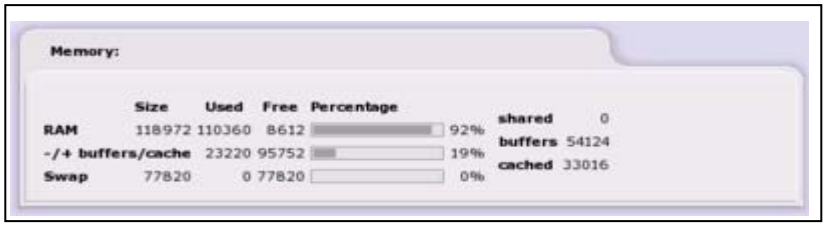
FIGURA 3.10 PROCESO DE CONFIGURACION PANTALLA Nro. 9



b) Memoria

Despliega el uso de la memoria en su servidor de IPCop.

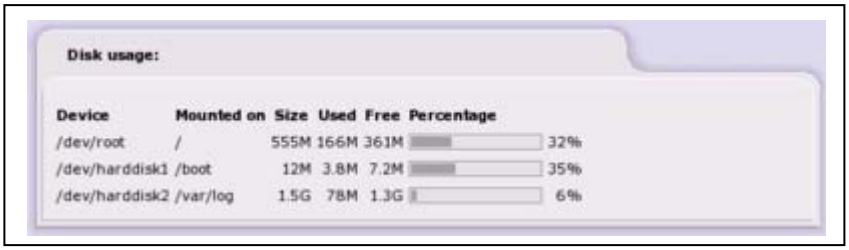
FIGURA 3.11 PROCESO DE CONFIGURACION PANTALLA Nro. 10



c) El uso del disco

Despliega el espacio total usado de la unidad de disco duro en su IPCop.

FIGURA 3.12 PROCESO DE CONFIGURACION PANTALLA Nro. 11



d) Usuarios

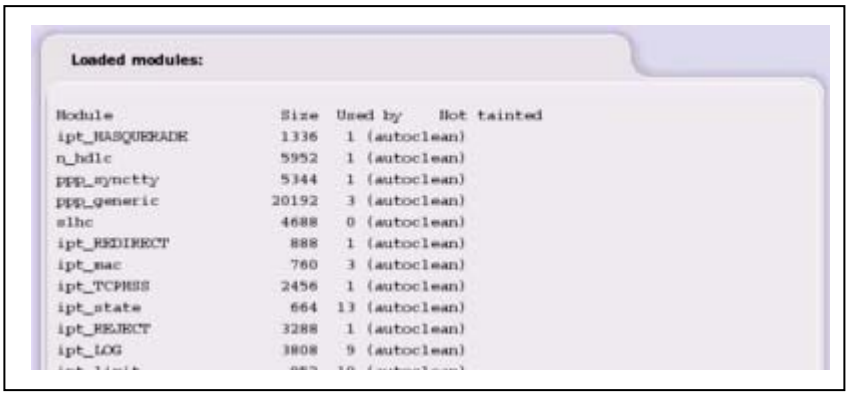
Despliega el rendimiento del orden del uptime e información de los usuarios que actualmente han ingresado en el servidor de IPCop.

FIGURA 3.13 PROCESO DE CONFIGURACION PANTALLA Nro. 12

e) Módulos cargados

Despliega todos los módulos actualmente cargados en el kernel.

FIGURA 3.14 PROCESO DE CONFIGURACION PANTALLA Nro. 13



f) Versión del Kernel

Despliega información sobre el kernel de IPCop.

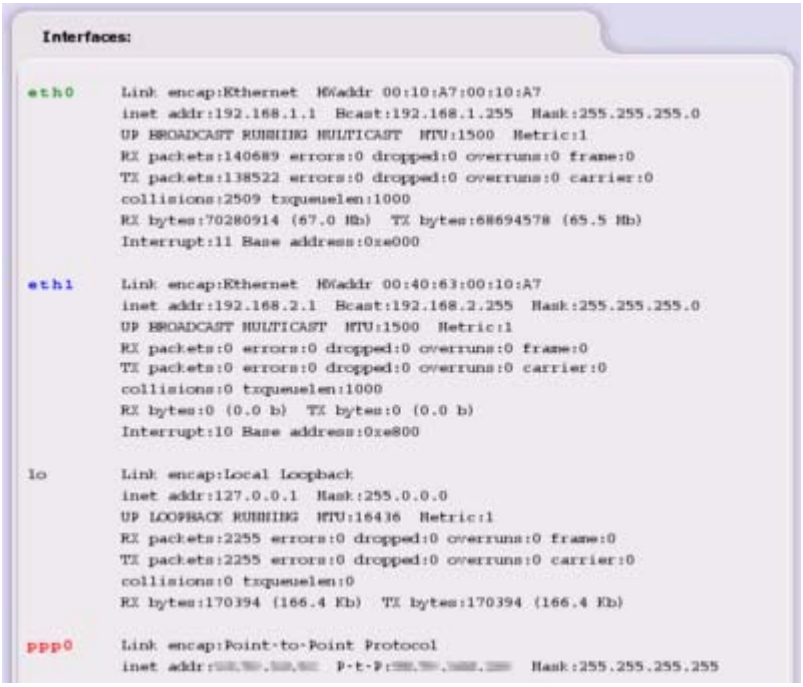
FIGURA 3.15 PROCESO DE CONFIGURACION PANTALLA Nro. 14

2. Estado de la Red

Esta opcion nos permite monitorear el estado de la red. Consta de la siguiente subdivisión:

a) Interfaces

Despliega información sobre todos los dispositivos de la red.

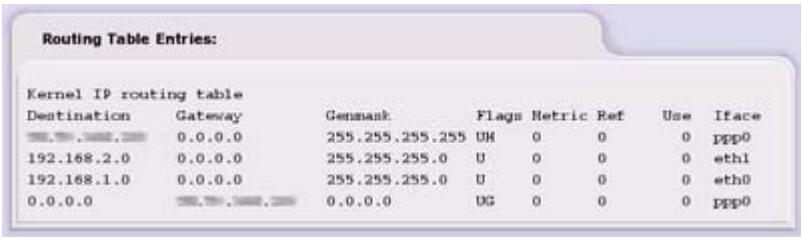


b) Current dynamic leases

Esta sección esta disponible solamente si DHCP esta habilitado. Despliega información acerca del IP address con su respectivo MAC address además el hostname y el vencimiento de las fechas para cada uno de los host.

c) Tabla de ruteo

Despliega la información de la tabla de ruteo de nuestra red.



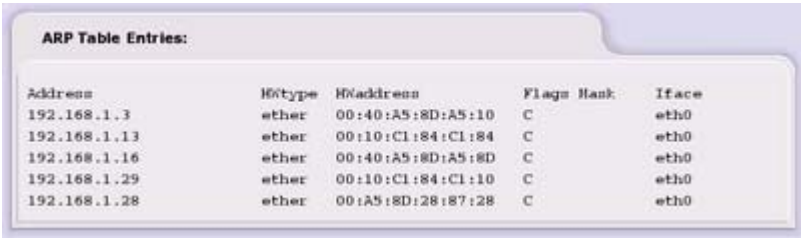
Routing Table Entries:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
[redacted]	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	[redacted]	0.0.0.0	UG	0	0	0	ppp0

d) Tabla ARP

Despliega la información de la tabla ARP que es la que permite a través de MAC address IP obtener la dirección IP.



ARP Table Entries:

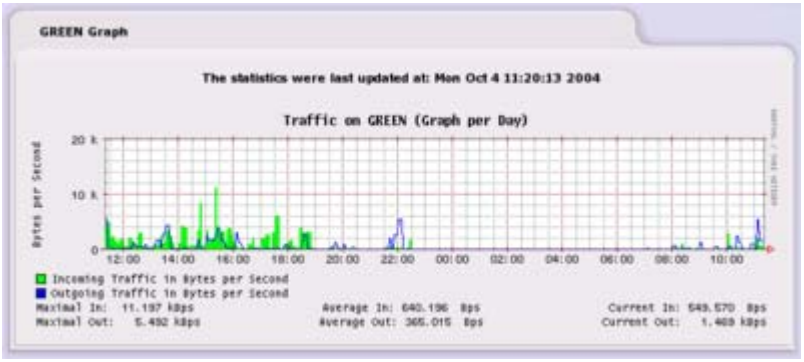
Address	HWtype	HWaddress	Flags Mask	Iface
192.168.1.3	ether	00:40:A5:8D:A5:10	C	eth0
192.168.1.13	ether	00:10:C1:84:C1:84	C	eth0
192.168.1.16	ether	00:40:A5:8D:A5:8D	C	eth0
192.168.1.29	ether	00:10:C1:84:C1:10	C	eth0
192.168.1.28	ether	00:A5:8D:28:87:28	C	eth0

3. Gráficos del Sistema

Esta opción nos permite visualizar los gráficos del uso por Día, Semana, Mes y Año de: Uso de CPU, Uso de Memoria, Uso del Swap y Uso del Disco

4. Gráficos del Trafico

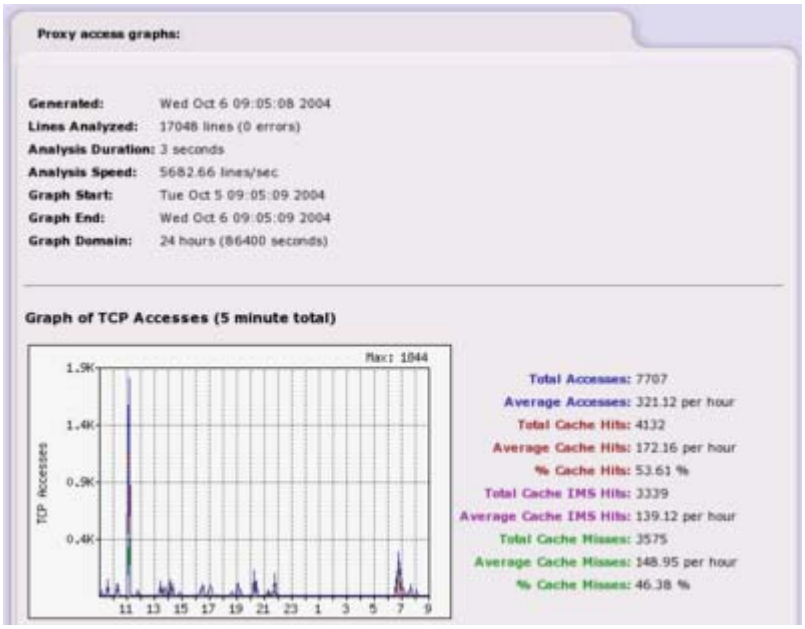
Esta opción permite tener una información gráfica del tráfico de nuestra red. Hay secciones para cada interfaz de la red, qué muestra gráficos de tráfico entrante y saliente a través de esa interfaz.



5. Gráficos del Proxy

   Esta opción muestra el tráfico a través del servicio Proxy del servidor IPCop.

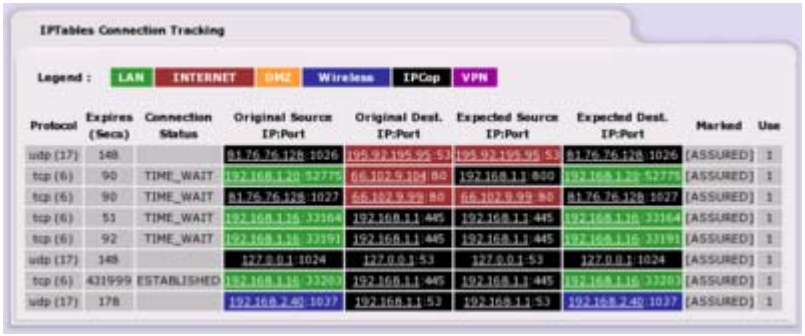
   La primera sección da la fecha y tiempo que el gráfico fue creado, el análisis de las líneas, la duración del el análisis, la velocidad (las líneas por segundo), la salida y fecha del fin, tiempo del gráfico, y el dominio (la longitud global del gráfico). Esta información es útil para ver si el tamaño del proxy.



6. Conexiones

   Esta opción guarda huella de las conexiones y de sus interfaces de red VERDE, AZUL y ANARANJADA, basándose en la fuente y destino las direcciones de IP y puertos, así como el estado de la propia conexión. Después de que una

conexión es establecida se involucra a las máquinas protegidas, y permite sólo paquetes seguros para el estado de la conexión mediante el uso del cortafuego de IPCop.



Menú Red:

Este menú presenta las diferentes opciones en caso de que se ocupe un proveedor de Internet vía MODEM.

Pruebas con cada una de las interfaces de red

Para las pruebas con cada una de las interfaces de red utilizaremos los siguientes menús:

Menú de Servicios:

IPCop puede proporcionar un número de servicios que son útiles en una red pequeña. Éstos son:

1. Web Proxy

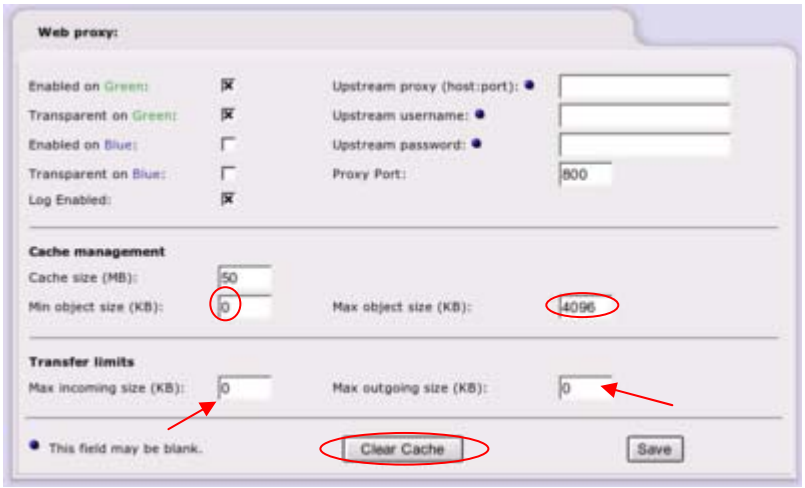
   Se debe configurar los navegadores web usados en su red para usar el servidor proxy para el acceso de Internet. Además debemos poner el nombre/dirección del proxy a la máquina de IPCop y el puerto predefinido como 8080.

Se puede habilitar el web proxy para permitir los accesos al log web marcando el campo **Log Enabled.**

En la segunda sección se puede escoger cuánto espacio del disco debe usarse para almacenar las páginas web. En la sección del manejo del cache podemos poner el tamaño del objeto más pequeño a ser guardado, normalmente 0, y el más grande, el 4096KB. Por razones de privacidad, el proxy no recibe las páginas del cache vía https, u otras páginas dónde un username y contraseña son enviados vía el URL.

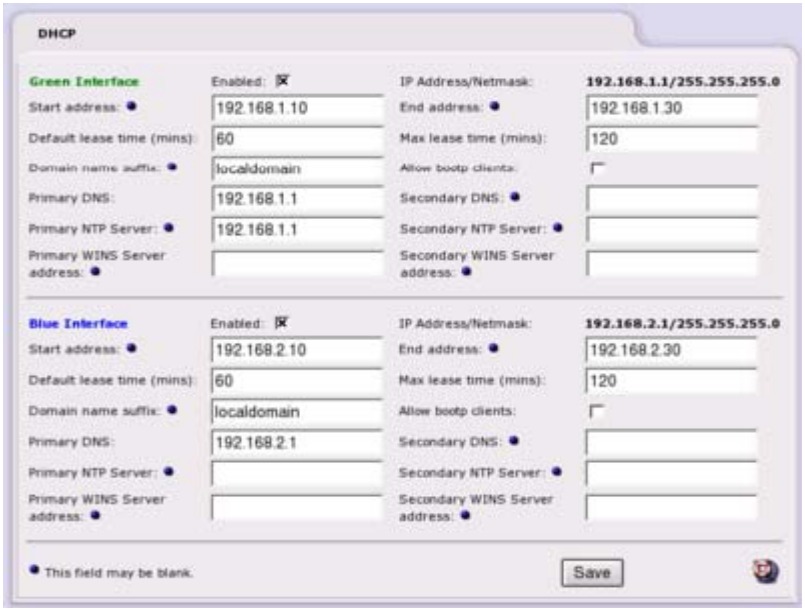
En la tercera sección se puede controlar los límites de transferencia de archivos es decir, controlar cómo sus usuarios acceden a la web y el tamaño máximo de los datos recibidos y enviados en la web. Nosotros utilizamos esta opcion para prevenir a los usuarios que transmiten archivos grandes y congestionen el acceso de Internet para todos los demás. Si no deseamos utilizar esta opción ponemos 0, para quitar todas las restricciones.

Para aplicar los cambios ponemos Guardar. Para vaciar todas las páginas fuera del cache del proxy pulsamos el botón Clear Cache.



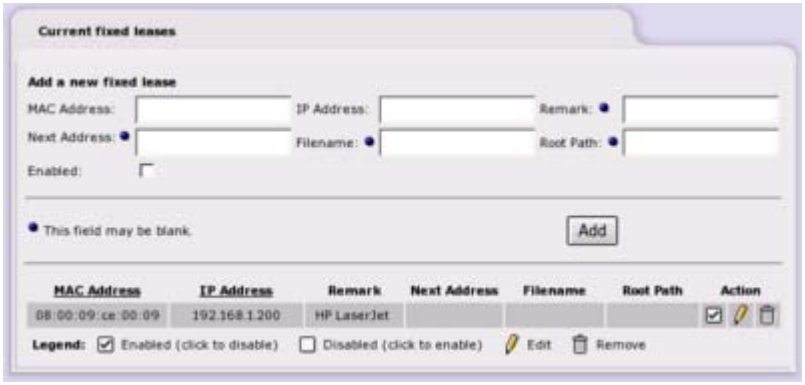
2. DHCP (obtener IP automáticamente)

   Esta opcion nos permite controlar la configuración de la red para todas las computadoras o dispositivos de nuestra máquina de IPCop. Cuando una computadora o un dispositivo se une a la red se dará una dirección IP válida y se pondrán su DNS de la máquina IPCop. Se deben configurar los parámetros de DHCP como se ilustra en el grafico.



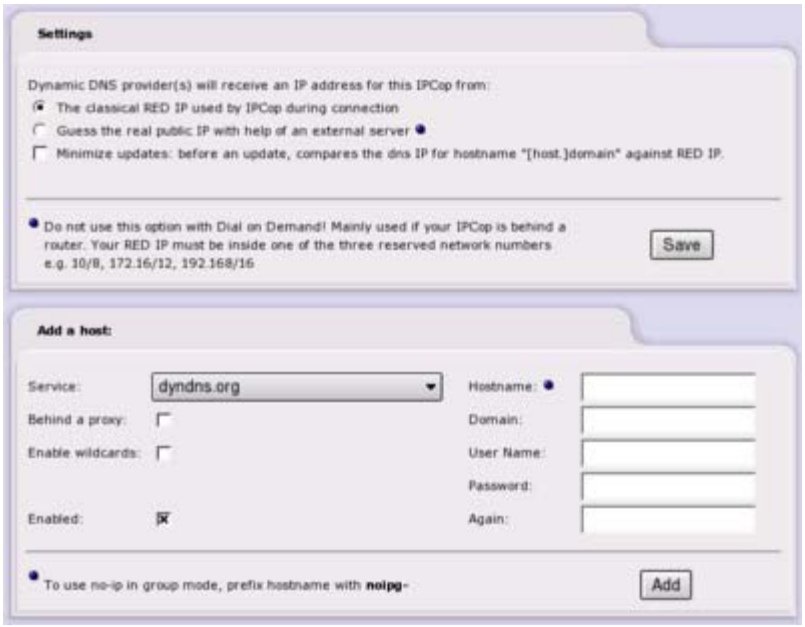
Existen opciones adicionales para cualquier parámetro especial que se quiera distribuir a su red vía el servidor de DHCP para esto se puede utilizar la siguiente pantalla:

Con el servicio DHCP podemos tener una dirección IP fija para cierta computadora que se conecte a nuestra red basada en la dirección de MAC para esto utilizamos la siguiente pantalla:



3. DNS dinámico

   Esta opción le permite hacer su servidor disponible a la Internet aunque no tiene una dirección IP estática. Cuando una máquina se conecta a su servidor se dará la dirección al servidor de DYNDNS que le dará el último el valor.



En la siguiente pantalla muestra las entradas de DYNDNS que usted ha configurado actualmente.

4. Trafico del Ancho de Banda

   Esta opción le permite priorizar el trafico IP movido a través de su cortafuego. Se utiliza para estimar la velocidad máxima en upload y download.

5. Intrusion Detection System Administrative Web Page

   IPCop contiene un sistema de descubrimiento de intrusión poderoso, analiza los volúmenes de paquetes recibidos por el cortafuego y búsquedas para las firmas conocidas de actividad malévola.

   IPCop puede supervisar los paquetes en las interfaces Green, Naranja Rojas. Sólo marcando las casillas de verificación y luego hacer clic en el botón Guardar.

Menú Firewall:

1. Reenvio de puertos

   Los cortafuegos impiden que las peticiones externas comiencen acceder el sistema protegido, esto significa que sólo usuarios de la misma red interna pueden usar el servidor web. Permite limitar el acceso a la LANs interior de afuera.

2. Acceso Externo

La opción de Acceso Externo no tiene NINGÚN efecto en las redes VERDES o ANARANJADAS. El campo Source IP, controla el acceso externo, si se deja ESPACIO EN BLANCO, estará abierto a TODAS LAS DIRECCIONES DE INTERNET. Alternativamente si usted pusiera una dirección, se restringirá a esa red o dirección de Internet.

Se puede tener más de una dirección externa, después de que ha creado la entrada del port forward, aparecerá en la tabla. Si se desea agregar otra dirección externa, pulsamos el botón el Lápiz Rojo con la señal + al lado de la entrada, la pantalla de la entrada de arriba, de la página cambiará y nos permite que entre un IP externo.

3. DMZ Pinholes

Esta opcion le permite configurar las DMZ Pinholes para IPCop, sólo será visible si se ha instalado y configurado una interfaz Naranja o Azul.
Los DMZ Pinholes o Zona Desmilitarizada (la zona Anaranjada) se usa como un punto del intercambio semi-seguro entre la Zona Roja externa y la zona interior Green.

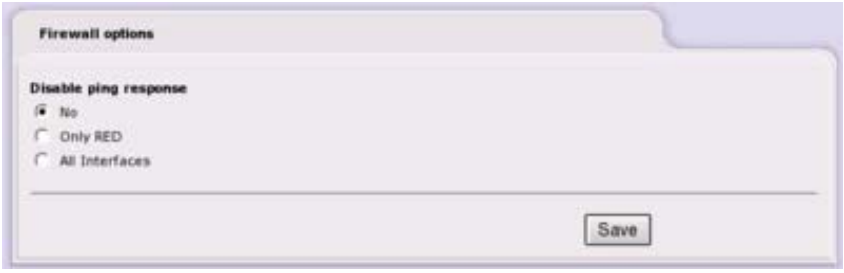
La zona Green tiene todas sus máquinas interiores. La zona Roja es la Internet. El DMZ nos permite compartir los servidores sin permitir el acceso indebido al LAN interior por otros en el La Zona roja.

4. Firewall Options

Esta opcion le permite configurar el comportamiento del cortafuego

Podemos desactivar la contestación del ping

- No: IPCop responde a las demandas del ping en cualquier interfaz. Éste es el comportamiento predefinido.
- Only ROJO: IPCop no responde a las demandas del ping en la Interfaz Roja.
- Todas las Interfaces: IPCop no responde a cualquier demanda del ping en cualquier interfaz.



Menú Logs:

1. Proxy Logs

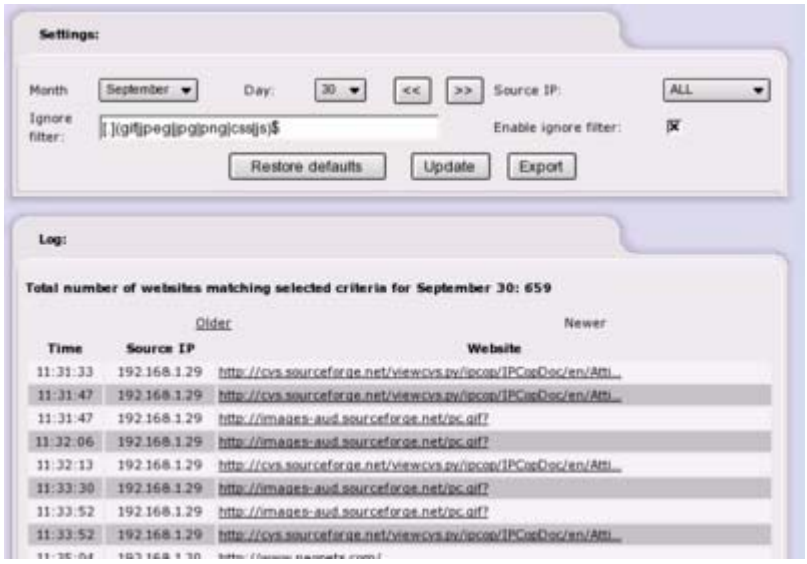
   Esta opción le proporciona la facilidad para ver los archivos que se han guardado el servidor del Web Proxy dentro de IPCop.

   Hay varios controles en esta página: del Mes, Día, y Actualización de los controles. La información de los que aparece en la pantalla consiste de:

   • El tiempo en el que el archivo fue guardado.

   • Source IP address de donde se abrieron los archivo.

   • El Website visitado.



2. Firewall Logs Page

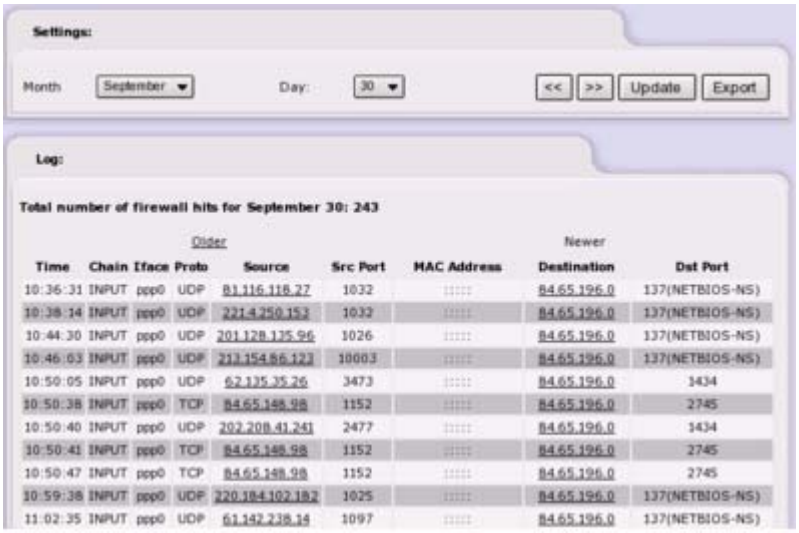
   Esta opción le proporciona la facilidad para ver los paquetes de datos guardado en el firewall. La información que contiene esta pantalla es la siguiente: Mes básico, Día, y le permite Actualizar o Exportar.

   En la sección Log contiene una entrada para cada uno de los paquetes que fueron bajados por el cortafuego. La información que contiene:

• El tiempo en el que el archivo fue guardado

• El Source y Destino IP al que se dirige y puertos para que pueda bajarse el paquete

• El IPCop Chain e Interfaz sean involucrados.



3. Instrusion Detection System Log Page

Esta opción nos muestra los incidentes detectados por IPCop, el sistema de Detección de Intrusión se activa en el menú de Servicios. La información que contiene son el Mes, Día, y nos permite Actualiza y Exportar.

Éstos le permiten examinar los Logs de IDS durante un día específico. Estos Logs consisten tienen varios artículos de cada incidente, la pantalla nos muestra la siguiente información:

• Fecha del incidente.

• Nombre: Descripción del incidente.

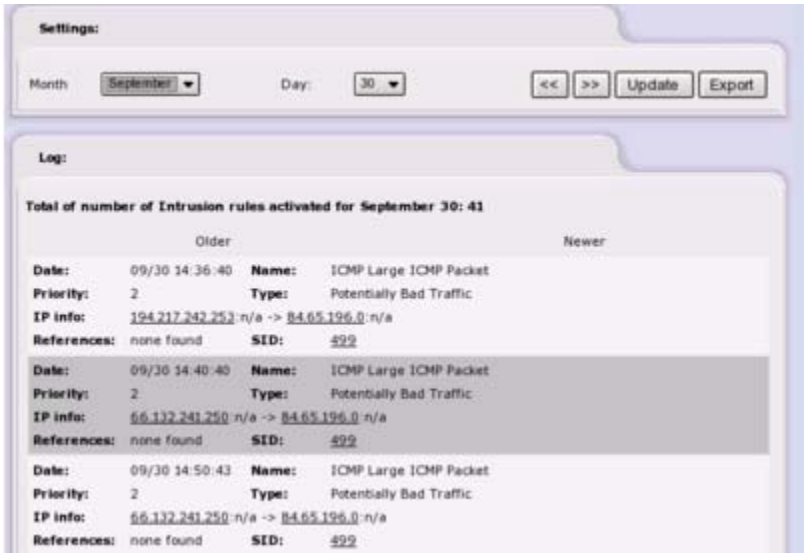
• Prioridad: Ésta es la severidad del incidente, evaluada así 1 ("malo"), 2 ("no demasiado malo"), y 3 ("posiblemente malo").

• Tipo: Descripción general del incidente.

• IP Info: Identidades de IP (la dirección y el puerto) involucradas en el incidente.

• Referencias: Hipervínculo a cualquier fuente disponible de información para este tipo de incidente.

• SID: - el Snort ID es el módulo del software usado por IPCop para proporcionar los IDS que funcionan, y también se utiliza para identificar un modelo particular de ataque.



4. Página de los Logs del Sistema

CONCLUSIONES

Podemos decir que el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro sin embargo, existen maneras de proteger las PC's contra amenazas y espías el proyecto IPCop es una de ellas. Luego de haber realizado las pruebas correspondientes estamos seguros que la aplicación correctamente instalada y configurada permite brindar esta seguridad a un bajo costo y con resultados efectivos los mismos que pueden ser aplicados para el bienestar y surgimiento de su empresa.

CONCLUSIONES GENERALES

Creemos que IPCop puede ser una muy buena solución para particulares o pequeñas empresas que requieran una eficaz protección de su red y no dispongan de un gran presupuesto, con este producto de licencia gratuita se puede reciclar hardware obsoleto y tener un sistema confiable que además puede utilizarse como Proxy, DHCP y hasta permite la comunicación por medio de VPN que podría ser útil para intercambiar datos entre sucursales.

Además hay que tener en cuenta que últimamente el mercado tiene una gran tendencia hacia el Software Abierto, y creemos que esta tendencia seguirá creciendo ya que entre otras ventajas es mucho más económico que el software cerrado.

REFERENCIAS

Glosario

IDS (Intrusión System Detection) Sistema de Detección de Intrusión

Bibliografía

MÍNIMO 10 REFERENCIAS EN ORDEN ALFABETICO

- ADMINISTRATIVE GUIDE IPCop, Clancey Chris, Goldschmitt Harry, Kastner John, Oberlander Eric, Walker Peter, 20 Septiembre 2004
- ARROYO, Cristian R. INSTALANDO IPCop EL FIREWALL HECHO MINIDISTRO. Vivalinux. 2000-2006.
- ELORREAGA MADRIGAL, Daniel Ramón. FIREWALLS Y SEGURIDAD EN INTERNET. www.monografías.com. México. s.a.
- EL FIREWALL PERFECTO EN LINUX IPCop. www.vampsecure.com. Febrero 2006
- GET SMOOTHWALL. 2000-2006.
- INSTALLATION MANUAL IPCop v1.4.0, Walker Peter, Goldschmitt Harry, and Pielschmidt Stephen ,2002-2004
- IPCOP-Y-SQUIDGUARD. www.bicubik.net. 2006
- KRIPTOPOLIS. CONSTRUYE TU PROPIO CORTAFUEGOS IPCop. 1996-2006.
- PCWORLD ECUADOR. Septiembre 2000. Número 211,
- QUICK STAR IPCop, Goldschmitt Harry, Marzo 2004

ANEXOS