Implementación y administración de Firewall IPCop en Grupo Fame

Autor: Yolanda Cruz García

Monografía presentada para obtener el título de:
Ing. En Sistemas Computacionales

Nombre del asesor:
Aldo Israel Sandoval Monroy

UNIVERSIDAD VASCO DE QUIROGA

FACULTAD DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

"IMPLEMENTACIÓN Y ADMINISTRACIÓN DE FIREWALL IPCOP EN GRUPO FAME"

MONOGRAFÍA

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN SISTEMAS COMPUTACIONALES

PRESENTA

YOLANDA CRUZ GARCÍA

ASESOR

ALDO ISRAEL SANDOVAL MONROY

CLAVE: 16PSU0049F

ACUERDO: LIC100846

MORELIA, MICHOACÁN

OCTUBRE-2012

ÍNDICE

RESUMEN

En los últimos años Internet ha revolucionado la forma de ver al mundo, lo cierto es que con ello, también se ha puesto en riesgo la estabilidad de los sistemas por todo el contenido que en él es posible encontrar.

A media que avanza su distribución, ha sido necesaria la creación de software que proteja la información; entre otras medidas de seguridad a los equipos se ha recurrido al uso de los llamados Firewall.

La integración de los Firewall a Grupo Fame, surge como parte de las medidas de seguridad y control dentro de la empresa, de esta forma, se realiza la implementación de IPCop, software basado en Linux que brinda una amplia gama de posibilidades a la hora de conectar una red local a Internet. Entre otros, uno de los grandes beneficios que este programa presenta es que restringe el acceso a sitios en los equipos de la red sin instalar nada en éstos.

IPCop 1.4.20 es un software especializado en proxy que permite la filtración de contenido (http, ftp, https) e inspección de paquetes de acuerdo con las políticas de seguridad implementadas en la empresa.

IPCop se puede instalar en equipos con pocas características respecto al hardware y es sencillo de configurar; la configuración a elegir depende del uso final; para este propósito se hará uso de las interfaces *VERDE* y *ROJA*, por la verde entrará todo el tráfico de Internet y por la roja saldrá toda la información requerida pero ya filtrada.

En esta monografía se plasma el desarrollo de la integración de IPCop como medida de seguridad en los servicios que proporciona Internet y con esto asegurar el entorno informático, así como también optimizar el tiempo y recursos de la empresa.

PLANTEAMIENTO DEL PROBLEMA

En las agencias de Grupo Fame, el consumo de ancho de banda es muy alto debido al número de conexiones a Internet sin control en cada una de las estaciones de trabajo de la empresa, esto retrasa el tiempo de respuesta en la red.

Distracción de actividades, equipos lentos, desconexión de Internet, formateo de equipos por virus, eran el resultado de la falta de restricciones de los accesos a Internet.

Dentro del Grupo apenas 3 agencias del total, contaban con un servicio externo que controlaba los accesos mediante la implementación de equipos Fortinet; colocar este mismo sistema generaría un gasto considerable.

De esta forma, se plantea la instalación de Firewall IPCop en cada una de las agencias del Grupo que cumpliera con la misma función, pero usando Software Libre que no requiere recursos económicos para su implementación.

ANTECEDENTES

Grupo FAME es uno de los principales Grupos de venta automotriz en México, hoy en día comercializa 18 marcas de autos distribuidas en 26 agencias en los Estados de Michoacán, Querétaro y DF. Día a día busca la implantación de procesos y sistemas para beneficio de quien lo integra y así, cumplir con la misión de obtener la máxima satisfacción del cliente.

Sin embargo; en lo que se refiere a la estructura de sus sistemas, experimentan problemas de alto consumo en ancho de banda, perdida de información y distracción en páginas de ocio por parte de los empleados; esto se ve reflejado en el desempeño y atención al cliente cuando se trata de dar una pronta respuesta a sus solicitudes, entre las que se encuentran: cotizaciones vía web, respuesta de correos, envío y recepción de archivos con virus.

Debido a que la atención al cliente y la pronta solución a sus peticiones es la base del negocio, se recurre al uso de nuevas herramientas que proporcionen seguridad y control, motivo por el cual se han implementado sistemas que sean capaces de llevar a cabo dicha tarea y a un bajo costo.

OBJETIVOS

Objetivo General:

"Desarrollar una guía para la instalación y administración de Firewall IPCop como medida de seguridad en Grupo Fame".

Objetivos Específicos:

- Aplicación de Firewall IPCop a todas las agencias de Grupo Fame.
- Proteger recursos y datos.
- Reducir el consumo de ancho de banda.
- Bloquear la descarga de programas maliciosos.
- Monitorear acceso a sitios y conexiones.
- Controlar la asignación de dirección IP a la red.
- Restringir el acceso a sitios de ocio.
- Aprovechar equipos en estado obsoleto.
- Reducir costos.

ALCANCES Y LIMITACIONES

El alcance del presente es desarrollar un estudio del estado actual de Seguridad Informática, que continuamente no es tomado muy en cuenta y que en la realidad se conoce muy poco; así como también desarrollar una guía para el control de seguridad en los servicios de Internet; y de esta forma cubrir parte de la problemática que se tiene en cuestión de Seguridad Informática.

En cuanto a material se refiere, se cuentan con los medios necesarios para llevar a cabo la instalación de los equipos. Teniendo la disponibilidad de los equipos en forma inmediata en cada una de las agencias ya que no será necesario generar gastos.

Se pretende establecer normas para el acceso a sitios, aunque en algunos casos, los accesos seguirán libres por peticiones de los Directivos.

JUSTIFICACIÓN

El siguiente plan se propone partiendo de la realidad actual. Como personal de Sistemas, uno de los deberes es apoyar a las demás áreas y al mismo tiempo facilitar la integración de la tecnología en los diferentes niveles de la estructura de la empresa.

Como es evidente, el área de Soporte tiene un trabajo constante, pues responde a la prevención y a la solución de imprevistos. Uno de los principales objetivos es la protección de recursos y datos, por lo que es importante analizar y probar distintas herramientas para evaluar el rendimiento.

La tarea principal en relación a este tema, es tener un control dentro de la misma área que permita en primer lugar, establecer normas que no existían. Con la implementación de éstos Firewall se logra no solo tener el control de los accesos a Internet, si no también, estabilidad en la red y evitar la descarga descontrolada de programas y archivos que dañaban el software de los equipos constantemente.

INTRODUCCIÓN

Hoy en día las redes están presentes en muchos lugares por razones importantes, como compartir recursos e información y con ello abaratar costos, así como también facilitar el trabajo en grupo. Entre otras también se encuentran:

- Compartir información de una forma más rápida y eficiente mediante el envío electrónico de mensajes y archivos.
- Proporcionar formas de comunicación directa con personas que están en otra ubicación.
- Compartir bases de datos.
- Compartir el acceso a Internet.

La importancia de Internet no reside solamente en el número de máquinas interconectadas sino en los servicios que brinda, siendo una de las herramientas que se han explotado más dentro y fuera de las empresas. Esto implica que el tráfico en Internet se haya aumentado durante los últimos años, sometiendo a pruebas constantes la capacidad de las redes.

Los usuarios conectados a una red, tienden a consumir el mayor ancho de banda posible, debido a la cantidad de información y software que en ella pueden encontrar, como administradores de red se debe incrementar la seguridad para frenar ataques externos a una red, motivo por el que son implementados los llamados Firewall.

Esta monografía tiene como finalidad documentar la instalación y configuración de la aplicación de IPCop como medida de protección a los equipos y datos de la empresa, y a su vez sirva como base para el desarrollo de otros proyectos, así como ampliar el uso de los Firewall como medida de seguridad.

En la primera parte se dará una explicación de los términos generales de la aplicación y las ventajas que tiene el uso de este software.

Posteriormente, basándose en la aplicación empírica así como en la recopilación de datos de Internet, se describirá paso a paso la instalación, configuración y administración de IPCop.

Finalmente, será posible comprobar cómo IPCop es una herramienta muy útil y barata a la hora de prevenir ataques externos.

Capítulo 1 MARCO TEÓRICO

1.1 INTERNET

"Internet es una red que vincula millones de equipos repartidos por todo el mundo"[1]. Su historia se remonta al temprano desarrollo de las redes, y surge de la necesidad de un medio de transmisión que permitiera la comunicación entre distintas redes.

En poco tiempo, Internet ha revolucionado el modo en que los usuarios emplean los equipos. Hoy en día, muchas personas dependen diariamente de este medio para comunicarse con otros y para obtener la información que necesitan.

En la siguiente imagen se muestra la tendencia del uso Internet en varios países del mundo incluido México[2].

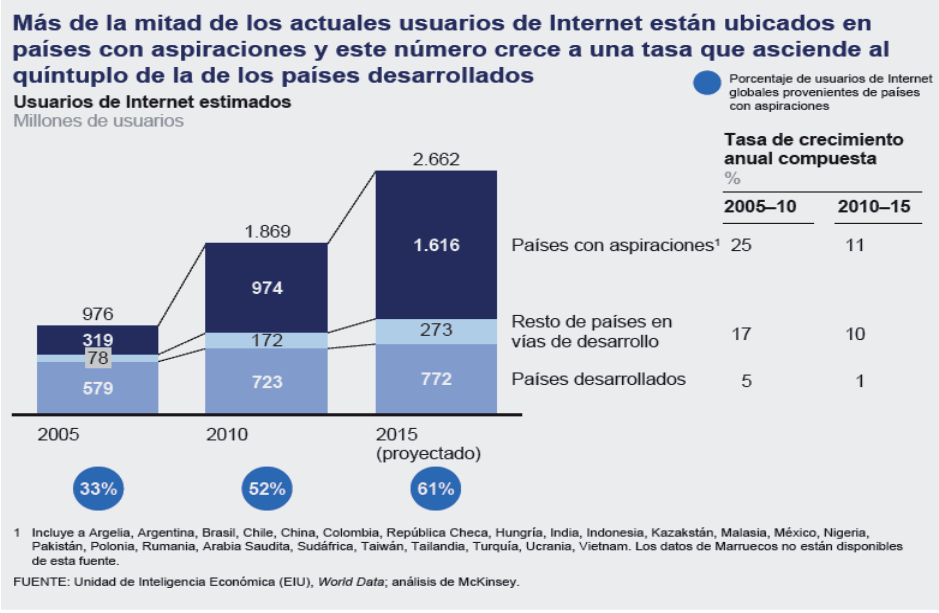


Fig. 1. 1 Tendencia del uso de Internet

[1] http://windows.microsoft.com/es-XL/windows-vista/Exploring-the-Internet
[2] En línea y en crecimiento: el impacto de internet en los países aspirantes: México. Análisis McKinsey 2012

El bajo costo y el intercambio casi instantáneo de las ideas se traduce en envío y recepción de millones de archivos que son transferidos diariamente. Para proteger los sistemas se han creado diversas herramientas para la protección de los equipos; una de éstas son los llamados Firewall.

1.2 FIREWALL

Un Firewall o puerto de seguridad es un dispositivo que forma parte de un sistema o una red cuya función es bloquear o filtrar el acceso entre dos redes, usualmente una privada (LAN) y otra externa (Internet). Los Firewall permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de ataques o virus a los sistemas.

De este modo un Firewall puede permitir desde una red local hacia Internet servicios de Web, correo y ftp, pero no a sitios de descargas o videos que pueden ser innecesarios para el trabajo de una empresa.

Riesgos que pueden controlar los firewalls:

- Uso oculto de los servicios de WWW y FTP desde dentro de la computadora. O riesgos externos desde la WWW.
- Aplicaciones ActiveX o Java Script instaladas clandestinamente, que son capaces de transferir datos personales del usuario a otros.
- Elementos de seguimiento como las cookies.
- Troyanos: aplicaciones ocultas que se descargan de la red y que pueden ser usadas por terceros, en forma remota, para extraer datos personales.
- Reducción del ancho de banda disponible por el tráfico de banners, pop up, sitios no solicitados, y otro tipo de datos innecesarios que ralentizan la conexión.
- Spyware: pequeños programas que se instalan con el fin de robar datos personales y espiar movimientos en la red.
- Dialers: programas que cortan la actual conexión y utilizan la línea para llamadas de larga distancia utilizadas por terceros.

Existen tres tipos de Firewall:

1. *Firewall de software:* Tienen un costo pequeño y son una buena elección cuando sólo se utiliza una PC. Su instalación y actualización es sencilla, pues se trata de una aplicación de seguridad, como lo sería un antivirus; de hecho, muchos antivirus e incluso el propio Windows poseen este tipo de Firewall.
2. *Enrutadores de hardware:* Su principal función es la de disfrazar la dirección y puertos de la PC a los intrusos. Suelen tener cuatro puertos de red para conexión mediante cableado.
3. *Firewall de hardware:* Son más caros y complejos de manejar en el mantenimiento y actualización. Los firewalls de hardware son más indicados en empresas y grandes corporaciones que tienen múltiples computadoras conectadas. También suelen utilizarse en aquellas empresas que prestan servicios de hosting y necesitan seguridad en los servidores.

1.3 LINUX Y SUS VENTAJAS

Linux es un Sistema Operativo basado en Unix que se distribuye bajo la GNU (Public License), por lo tanto, el código fuente tiene que estar siempre accesible.

Entre las ventajas del uso de este Sistema Operativo están:

- Linux es un Sistema Operativo gratuito.
- Al ser software libre, se incluye el código fuente, lo que permite modificarlo de acuerdo a las necesidades del usuario.
- Usa varios formatos de archivo que son compatibles con casi todos los sistemas operativos que se usan actualmente.
- El equipo donde corre el Firewall necesita requerimientos mínimos de hardware, por tanto es posible reutilizar equipo obsoleto.
- Sobre el sistema operativo Linux es posible montar múltiples servicios tales como:

- Servidor Proxy HTTP y FTP con cache de disco para acelerar la navegación por Internet.
- Informes generados en forma automática, gráficos de monitoreo (CPU, RAM, SWAP, Tráfico de red).
- Bloqueo opcional para la navegación en más de 30.000 sitios.
- Conversión de las direcciones IP de su red privada (NAT).

Las tecnologías de información ofrecen una amplia gama y diversas soluciones tecnológicas cuyo nivel de eficiencia y competencia cada día se compara más. Resultando que cada vez más empresas elijan el software libre, no solo por ser un sistema gratuito; sino también, por su alta fiabilidad, ya que Linux presenta gran calidad y estabilidad.

1.4 IPCOP, QUE ES Y PARA QUE SIRVE

IPCop es una distribución Linux que implementa un Firewall y proporciona una sencilla interfaz web de administración. Está orientado a usuarios domésticos o a pequeñas empresas (SOHO). Originalmente nació como una extensión (fork) de la distribución SmoothWall.

IPCop es un proyecto GNU/GPL. Se trata de un Firewall basado en Linux que brinda una amplia gama de posibilidades a la hora de conectar una red local a Internet.

Fig. 1. 2 Logotipo IPCop

Un Firewall es sencillamente un filtro capaz de controlar y examinar todas las comunicaciones, entrantes y salientes, que pasan de una red a otra permitiendo o denegando las transmisiones y vigilando todos los puertos de red.

1.4.1 Topologías de red soportadas

IPCop permite la implementación de diferentes topologías de red, ya sea desde la simple LAN que sale a Internet, hasta la creación de una zona desmilitarizada (DMZ), soportando también la inclusión de una red inalámbrica.

Permite gestionar el acceso a Internet, la seguridad y la interacción de hasta cuatro redes distintas, con las siguientes características:

- RED: Zona de Internet.
- GREEN: Red de Área Local (LAN) cableada.
- ORANGE: Zona desmilitarizada (DMZ, para la granja de servidores).
- BLUE: Zona inalámbrica (Wireless).

ROJA (RED): Es la interfaz de red que se conectará directamente al proveedor de Internet. Puede ser una conexión ADSL, cable modem ó una línea dedicada. Cualquier instalación de IPCop contará con esta interfaz habilitada. (Soporta tanto dispositivos Ethernet como USB).

VERDE (GREEN): Esta es la interfaz de red de la LAN. Aquí es donde se conectarán todos los equipos que necesiten mayor protección, como servidores que no tengan presencia en Internet y puestos de trabajo; se presume que detrás de esta interface habrá tráfico local que para acceder a otras redes deberá pasar por IPCop.

NARANJA (ORANGE): Esta es la interfaz que se utilizará para montar una DMZ o zona desmilitarizada. Principalmente se utiliza para montar servidores web, de correo, de ftp, etc. que deban ser accesibles desde Internet, pero que en el caso que se produzca alguna intrusión a algún equipo de esta red, no se comprometa la seguridad de la red interna (GREEN). Las computadoras en esta red no pueden comunicarse con las de las redes VERDE ni BLUE, excepto por intermedio de agujeros firmemente controlados de DMZ (zona desmilitarizada).

AZUL (BLUE): Es la interfaz que se asigna normalmente para conectar un Access Point de modo que se puedan conectar dispositivos inalámbricos. De todas maneras sirve para conectar cualquier otra red que se necesite sea esta inalámbrica o no. Los dispositivos que se encuentren en esta red, no podrán iniciar una conexión a los dispositivos que se encuentren en la interfaz VERDE, pero salvo esta excepción, contarán con el mismo nivel de acceso y protección que cuentan los dispositivos conectados a la interfaz VERDE.

Estas cuatro posibles redes no son más que cuatro placas de red en la misma PC. No es necesario utilizar las cuatro, sino que se puede configurar de diferentes maneras dependiendo de las necesidades que se tengan. Con IPCop se puede trabajar de formas distintas entre las que se encuentran:

- GREEN (RED is modem/ISDN).
- GREEN + ORANGE (RED is modem/ISDN).
- GREEN + RED (RED is Ethernet).
- GREEN + ORANGE + RED (RED is Ethernet).
- GREEN + ORANGE + BLUE.

El propósito primario de IPCop es proteger la red VERDE y NARANJA y sus equipos del tráfico originado en la red ROJA.

1.4.2 Modo de trabajo de IPCop

IPCop trabaja mediante IPtables, que es un sistema de Firewall vinculado al Kernel de Linux, esta tecnología permite el filtrado de paquetes a través de reglas, esto es posible mediante la ejecución del comando IPtables, con el que es posible añadir, borrar o crear dichas reglas.

En IPCop pueden establecerse un conjunto de reglas para cada tipo de interfaz (ROJA, VERDE, NARANJA y AZUL), puesto que cada una tiene asociado un determinado nivel de confianza en función del tipo de tráfico al que están expuestas. Así, la más restringida sería la Roja y la menos, la Verde.

Hay tres políticas de acceso para las interfaces, salvo excepciones - NARANJA abierta o cerrada, ROJA cerrada. Éstas son:

- Open: Acceso abierto a servicios de IPCop y cualquier otra interfaz.
- Half-Open: Acceso abierto a servicios de IPCop.
- Closed: Acceso completamente cerrado a la interfaz.

Si se necesita acceso a una interfaz con esta política, debe crearse una regla específica para dicho acceso. Se dispone de dos opciones de denegación de acceso, seleccionables por el administrador para ser llevadas a cabo al descartar un paquete. Son las siguientes:

- Drop: Descarta un paquete entrante de manera “silenciosa”, es decir, deniega el acceso pero no informa acerca del bloqueo.
- Reject: Descarta un paquete entrante y envía de vuelta un paquete ICMP. Se recomienda no utilizar esta opción en la interfaz Roja (Internet), ya que se expone el sistema a un posible ataque de denegación de servicio.

La instalación se basará en una política restrictiva, en la que se deniega todo el tráfico excepto el que está explícitamente permitido. El Firewall obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

1.4.3 Ventajas de IPCop

Estas son algunas de las principales características por las que se decidió implementar el software de IPCop:

- Seguro, Estable y altamente configurable.
- Web Server con páginas que permiten la sencilla administración del Firewall.
- Cliente DHCP que permite obtener la dirección IP automáticamente desde el ISP (Proveedor de Servicios de Internet).

- Servidor DHCP que permite una rápida y sencilla configuración de estaciones de trabajo en la red interna.
- Proxy DNS cache, que permite incrementar la velocidad de resolución de consultas de nombre de dominio.
- Detección de intrusos para advertir ataques desde la red externa.
- VPN que permite que se conecte la red interna con otra red a través del Internet, formando una sola red lógica.
- Permite la integración de módulos adicionales Add-on, que amplían el uso la herramienta.

1.4.4 Los Add-on

Existen varios desarrolladores (sin vinculación con el equipo de desarrollo de IPCop) que han desarrollado paquetes con funcionalidad adicional, que se denominan Add-on. Estos permiten una amplia gama de funcionalidades no incluidas originalmente en el producto. A continuación se señalan algunas de las características de cada uno de los Add-on que fueron seleccionados para la instalación:

AdvProxy

Este Add-on es un potente proxy que permite controlar las conexiones salientes de la red hacia Internet. Entre sus capacidades se encuentran:

- Autenticación de usuarios locales, incluyendo administración de grupos de usuarios.
- Acceso a subredes permitidas.
- Administración Extendida de la cache.
- Control de Acceso Web por IP y dirección MAC.
- Restricciones basadas en accesos por tiempo.
- Restricciones de descarga y subida (tamaño de éstas).
- Bloqueo de navegadores o clientes.
- Filtrado MIME.

UrlFilter

La función de este Add-on es controlar a que acceden los usuarios a Internet, entre sus funciones se encuentran:

- Completa integración con la Interfaz Gráfica de Usuario para la configuración y la visualización de los Logs.
- Bloqueo de dominios no deseados, direcciones URL mediante filtrado por categorías, así como archivos según su tipo.
- Trabaja con todas las listas negras compatibles con SquidGuard.
- Actualizaciones de las listas negras dinámicas y programadas.
- Selección de horarios en los que serán efectivas las reglas.

Calamaris

Con este Add-on se generan reportes para el proxy, sus características incluyen:

- Peticiones entrantes (TCP y UDP), y salientes.
- Peticiones de dominios de primer y segundo nivel.
- Reporte de Protocolos (http, gopher, ftp, …).
- Peticiones según tipos y extensión de ficheros.
- Distribución basada en el tamaño de los objetos.
- Rendimiento en rangos de tiempos definidos.

BlockOutTraffic

BlockOutTraffic (BOT) es un Add-on que bloquea todo el tráfico que se permite en una instalación de IPCop normal, sus características son:

- Completa integración a la Interfaz Gráfica de Usuario.
- Control del tráfico hacia y a través de IPCop.

- Restricciones del tráfico por direcciones MAC, IP e interfaces de red.
- Agrupación de direcciones para una mayor organización.
- Definición de servicios personalizados.
- Agrupación de servicios.
- Reglas de tiempo basadas en el Firewall.
- Control de los log de Firewall.
- Normas sobre el tiempo del Firewall.

Updatex

El uso de este Add-on es muy útil ya que las actualizaciones de Windows Update, entre otros, se realizan directamente desde IPCop y no consumen ancho de banda, además:

- Almacena en caché los archivos desde sitios de actualización de forma automática en la primera solicitud. Todas las descargas posteriores serán descargadas a la velocidad de la LAN, lo que permite ahorrar tiempo.
- Entrega garantizada de la caché local, incluso si la caché de proxy web ha sido borrada.

P2P Block

La función primordial de este complemento es bloquear todo el tráfico P2P en la red. De tal forma que programas como Ares, Kazaa, Emule, BitTorrent, entre otros. No podrán realizar conexiones.

En el siguiente capítulo se describe el proceso de instalación, configuración y administración de IPCop, que va desde la instalación básica, integración de los Add-on y aplicación de reglas.

Capítulo 2 INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN DE IPCOP

2.1 ESPECIFICACIONES TÉCNICAS

En el siguiente capítulo se especifican los requisitos para llevar a cabo la instalación del Firewall, así como la configuración que debe llevar enfocada a las solicitudes de Grupo Fame.

2.1.1 Requisitos de hardware

Respecto al hardware necesario para la instalación de IPCop, se puede decir que corre en casi cualquier equipo; sin embargo, para instalar los Add-on, lo más recomendable es utilizar hardware con mayores características.

Para llevar a cabo la instalación de los firewall se busco hardware relativamente obsoleto para ser aprovechado. De esta forma, se utilizaron equipos con las siguientes características:

- Procesador Pentium IV
- 512 Mb en RAM
- 40 Gb en disco duro
- 1 tarjeta de red 10/100 adicional a la que incluye la placa base, previamente instalada.
- Unidad CD

Aunque puede ser ejecutado en equipos con menores características; se eligieron estas características por los módulos adicionales (Add-on) que se van a instalar.

2.1.2 Software para instalación y configuración de IPCop

Para llevar a cabo la instalación y administración de IPCop desde la misma red o desde internet se utilizarán una serie de programas.

IPCop se puede descargar desde el sitio oficial[3], consiste de una imagen ISO de aproximadamente 50Mb la cual puede ser grabada en un CD. La versión que será instalada es la 1.4.20.

La configuración Web se podrá realizar desde cualquier navegador como Internet Explorer, Mozilla ó cualquier otro.

Para tener acceso a la consola será usado PuTTY. Programa SSH que servirá como interfaz entre IPCop y otra máquina.

La transferencia de archivos se llevará a cabo mediante WinSCP, aunque puede usarse también Filezilla, FireFTP, entre otros.

Para ampliar la gama de funcionalidades no incluidas originalmente en el sistema, se hará uso de paquetes, llamados Add-on. Entre la variedad de Add-on disponibles, deberán ser descargados los siguientes:

- Advproxy 3.0.6
- BlockOutTraffic 3.0.0
- Calamaris 2.1.2
- Updatex 2.1.3
- UrlFilter 1.9.3
- P2P block 1.4.21

Estos archivos se deberán descargar comprimidos y se colocarán en una carpeta con nombre Addons.

[3] http://www.ipcop.org/download.php

2.1.3 Selección de Interfaces

En el capítulo anterior se explican las diferentes configuraciones con las que se puede trabajar en IPCop, así que antes de comenzar la instalación se debe elegir la topología de la red que cumplirá con los requisitos.

De acuerdo al esquema de red dentro de las empresas, la configuración de tarjetas que se adecua a este propósito es:

VERDE (Green) + ROJA (Red)

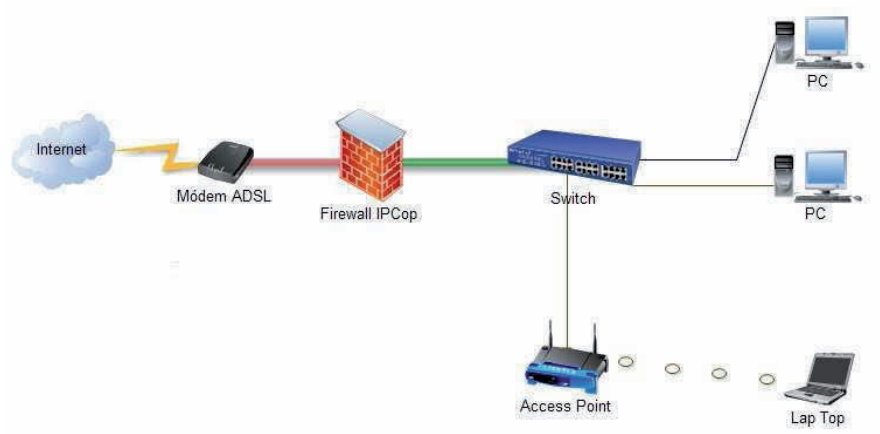


Fig. 2. 1 Conexión de dispositivos en la red de Grupo Fame

De esta forma, la interfaz ROJA (Red con IP dinámica) se comunicará por medio de un MODEM a Internet. Y por otro lado estará la VERDE (Green con IP Fija), que estará conectada al Router o switch de la red local (LAN) que se desea proteger.

2.2 INSTALACIÓN

La instalación de IPCop es relativamente sencilla una vez que se ha definido la configuración inicial. A continuación se detalla el procedimiento que habrá que llevar a cabo.

Antes de iniciar, se recomienda ingresar a la BIOS para configurar el equipo en caso de un corte de energía, éste vuelva a iniciar al regreso de la misma.

Con el disco de instalación en el CD-ROM se enciende el equipo, esto provoca que se active el LILO (Linux Loader) y se muestre la siguiente pantalla.

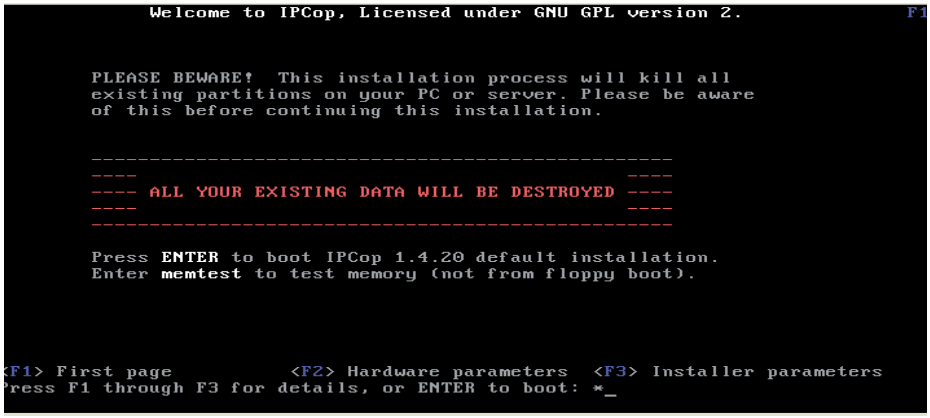


Fig. 2. 2 Inicio de instalación IPCop

La primera pantalla es una advertencia de que la instalación eliminara todas las particiones existentes y se perderán todos los datos. Para continuar se presiona la tecla ENTER.

Luego de confirmar la instalación, el sistema ejecuta el software instalador de IPCop y solicita la selección del idioma en el que se instalara.

Fig. 2. 3 Selección de idioma

Posteriormente da la bienvenida al programa e indica que si se cancela el equipo será reiniciado.

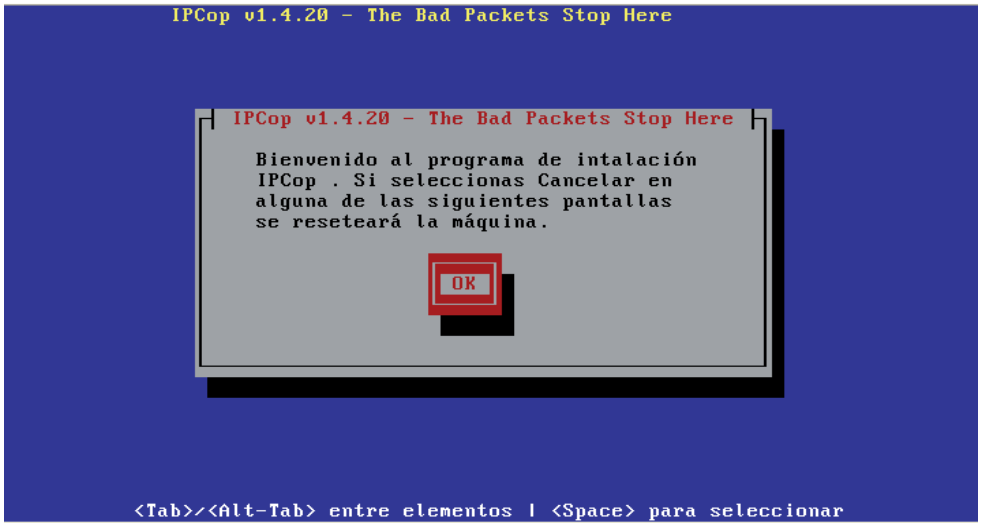


Fig. 2. 4 Bienvenida al programa de instalación

El siguiente paso es seleccionar el medio con el que se llevará a cabo la instalación, en este caso, se selecciona CDROM. De esta forma empecerá a ejecutarse el programa instalando los ficheros y haciendo la prueba de los discos.

Fig. 2. 5 Modo de instalación

IPCop permite restablecer copias de seguridad, si se tuviese alguna falla habría que seleccionar el medio, el nombre del host y la contraseña e IPCop recuperara los archivos; como se inicia con una nueva instalación, se selecciona Saltar.

Fig. 2. 6 Restablecer

El sistema realizará las pruebas de detección de tarjetas, primero buscará la que se designará como interfaz verde con los drivers proporcionados.

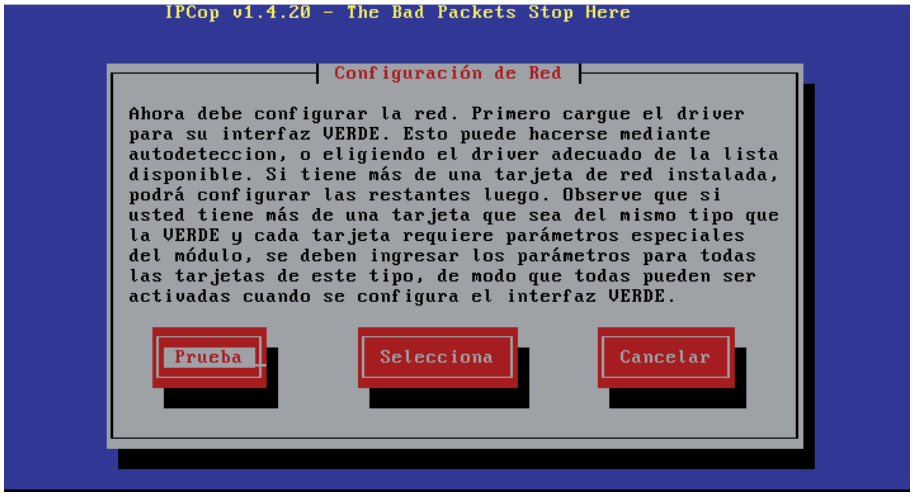


Fig. 2. 7 Configuración de red

Una vez que detecta la red, solicita la dirección de IP y la correspondiente mascara de subred para dicha interfaz, esta dirección será la que verá al firewall desde la red local.

Fig. 2. 8 Configuración de la interfaz Verde

Posteriormente solicita la extracción del CD para comenzar con el setup que permitirá la configuración del resto de tarjetas así como las contraseñas.

2.3 CONFIGURACIÓN

En esta sección se explica cómo se realiza la configuración estándar de la distribución, en la primera parte se verá la configuración inicial que es la que se realiza en el momento posterior a la instalación, luego se realizará la configuración vía web por medio de https.

2.3.1 Configuración inicial

Esta es la configuración que se lleva a cabo en el momento posterior al proceso de instalación.

Lo primero que solicita es la información básica como la configuración del teclado, la zona horaria, el nombre del equipo, y el dominio.

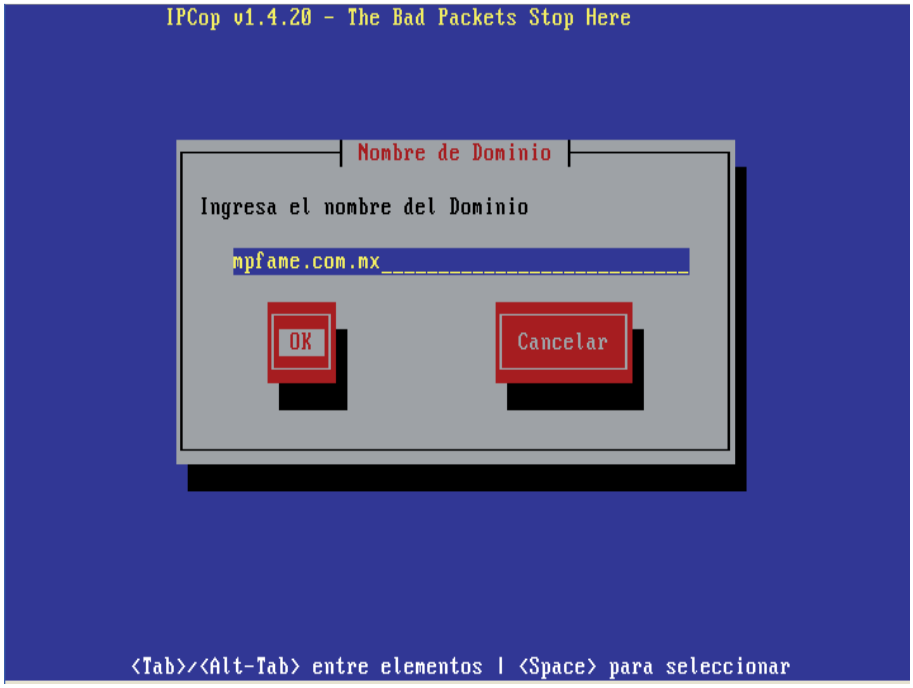


Fig. 2. 9 Nombre del Dominio

A continuación se despliega la pantalla de configuración de ISDN. En este caso, esta pantalla no es de utilidad, debido a que no se poseen dispositivos ISDN (RDSI).

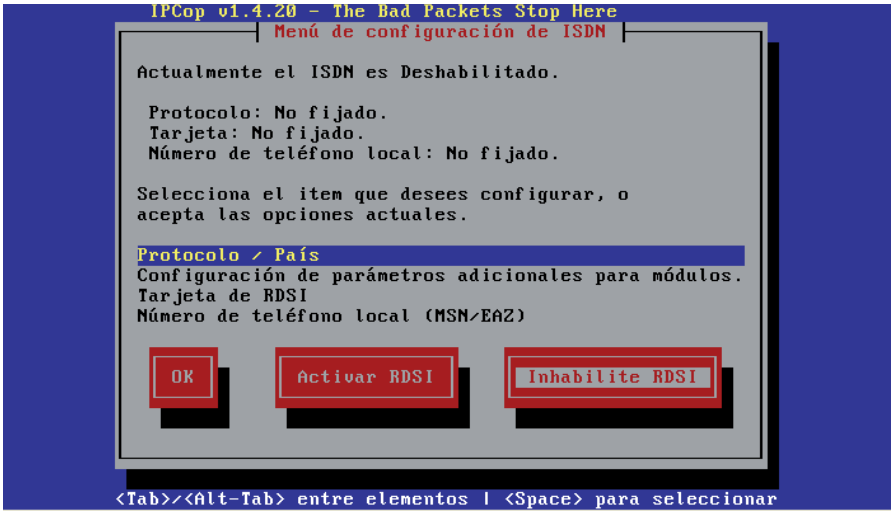


Fig. 2. 10 Menú de configuración de ISDN

Tipo de configuración de red. Este fue el que se definió al inicio.

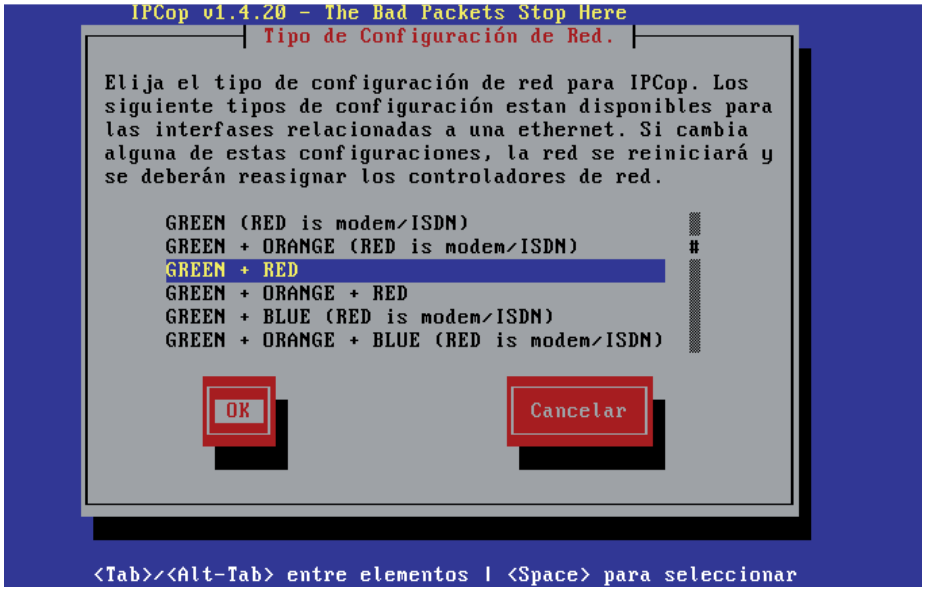


Fig. 2. 11 Tipo de configuración de red

Controladores y tarjetas asignadas. Muestra la tarjeta asignada, pero aún hace falta que el programa identifique la segunda para asignarla a RED.

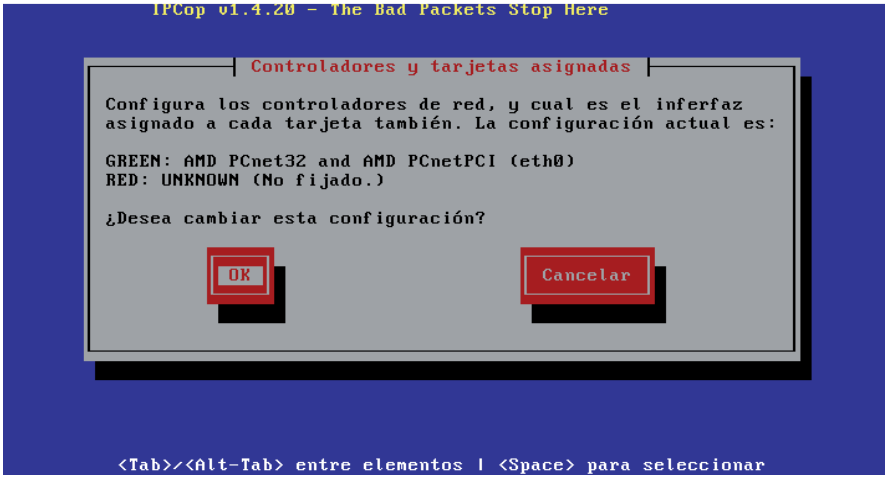


Fig. 2. 12 Controladores y tarjetas asignadas

Una vez que la identifica, la asigna, enviando un mensaje que indica que las tarjetas se asignaron con éxito, el motivo por el que no llegara a encontrar el controlador puede deberse a que la tarjeta de red no es compatible.

Lo siguiente es configurar la interfaz RED, para este caso, tendrá una IP dinámica al seleccionar PPPOE, debido a que el cable de esta interfaz será directamente conectado al módem.

Fig. 2. 13 Configuración de la interfaz Roja

Opciones de DNS y Gateway. En este paso se configuran las opciones que tomara la estación de trabajo de la red VERDE.

Fig. 2. 14 DNS y Gateway

Configuración DHCP. Esta opción se desactiva si se requiere que la red tenga un rango de IP fijas, este caso, se activa para que el servidor asigne las IP por DHCP.

Fig. 2. 15 Configuración del servidor de DHCP

Una vez finalizada la instalación se solicitarán las contraseñas de acceso a la administración de IPCop, siendo estos:

- ROOT: Usuario utilizado para el acceso mediante la consola de comandos.
- ADMIN: Usuario para acceder vía Web.
- BACKUP: Usuario para exportar los respaldos del sistema.

Fig. 2. 16 Contraseñas de acceso

El sistema pide reiniciar, quedando una pantalla negra con un “login”, para entrar, bastará con indicar el usuario root y la contraseña con anterioridad establecida, si por algún motivo se necesitara reconfigurar IPCop se podrá hacer mediante el comando “setup”. A partir de este momento el firewall puede verse desde la red local.

2.3.2 Instalación de los Add-on

Antes de instalar los Add-on es necesario activar algunas opciones y actualizaciones desde Web. Desde cualquier equipo de la red local, habrá que abrir el Navegador Web e ingresar la dirección de la interfaz VERDE por medio del protocolo https en el puerto 445. En este caso es https:\\192.168.4.253:445.

Una vez dentro del sitio aparecen las fichas que a su vez contienen los menús. En cuanto se trate de ingresar a una de éstas, el sitio solicitará los datos que fueron definidos en el usuario ADMIN.

Fig. 2. 17 Login acceso Web

Para poder realizar la descarga de las actualizaciones es necesario que el equipo esté conectado a internet, para ello es necesario tener conectadas las dos interfaces de IPCop, al entrar a la interfaz HTTPS la primera página que se muestra indica que la configuración no es

la correcta, esto se debe a que la interfaz ROJA aún no tiene comunicación, para corregir esto, en la ficha *Red/Marcado* se configura de la siguiente forma:

- Interfaz: PPPOE.
- Conectar al reiniciar IPCop, es importante la selección para no hacerlo manual en cuanto IPCop se reinicie.
- Reconexión persistente.
- Configuración Adicional: PPPOE.
- Autenticación: Indicar nombre de usuario y contraseña, esta información la proporciona el proveedor de servicio de internet.
- DNS: Automático.
- Asignar nombre al perfil.
- Guardar.

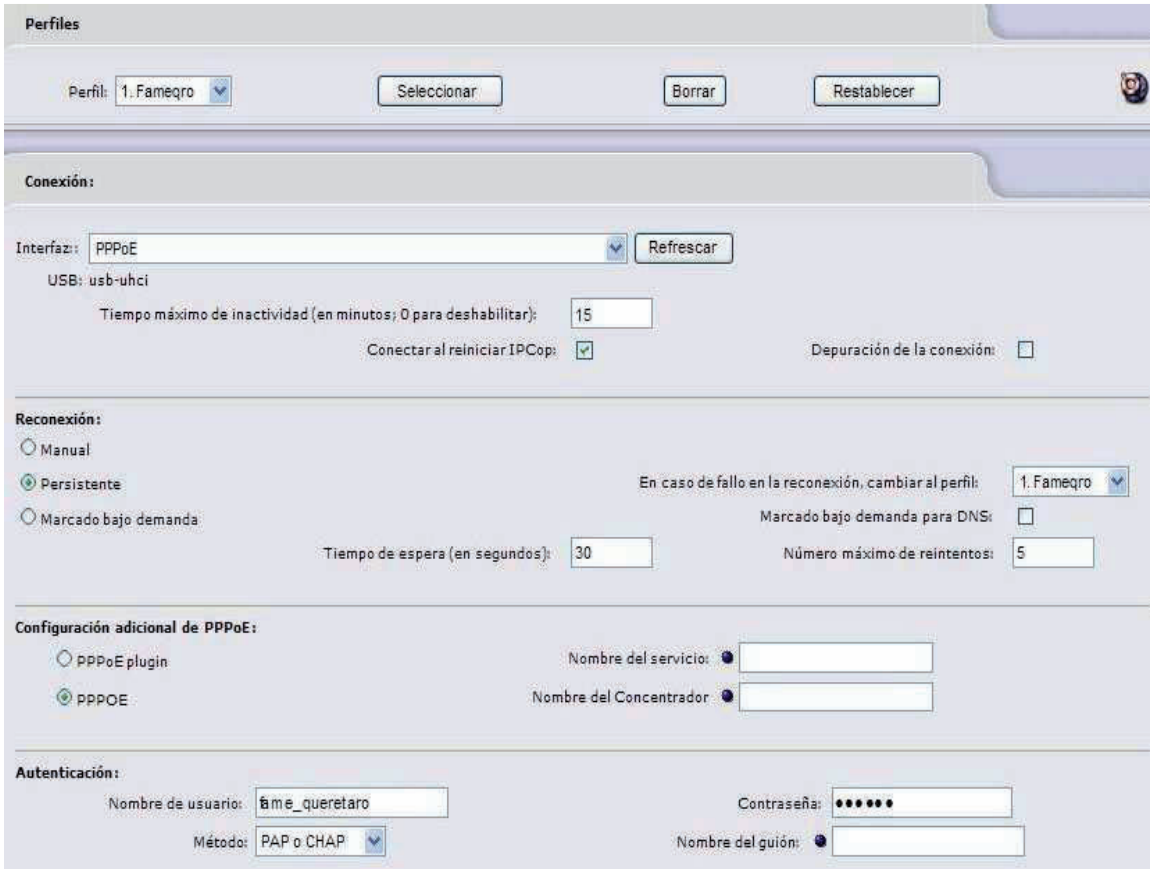


Fig. 2. 18 Configuración de conexión tarjeta roja por PPPOe

A continuación, se realizará la actualización del sistema, esto con la finalidad de ejecutar adecuadamente el Add-on P2P Block. En la ficha *Sistema/Actualizaciones* aparece una actualización disponible 1.4.21, al descargarse y ejecutarse, el sistema lo indica.

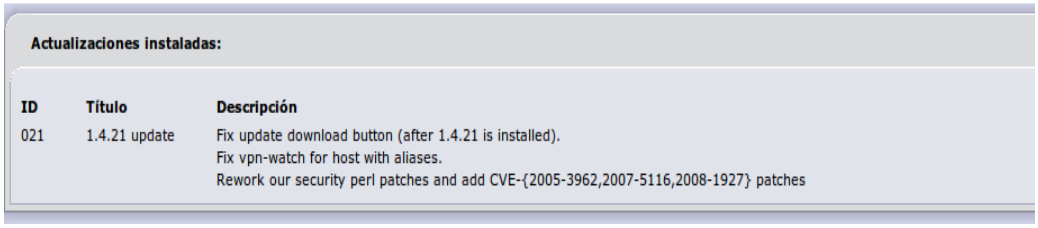


Fig. 2. 19 Actualizaciones instaladas

IPCop permite su administración mediante SSH, los programas para llevar a cabo este propósito son WinSCP y Putty; sin embargo, para poder usarlos habrá que activar el acceso SSH, está opción se encuentra de la ficha *Sistema/Acceso SSH*, se selecciona Acceso SSH y se guarda el cambio. En esta misma página indica que el puerto para la conexión es el 222.

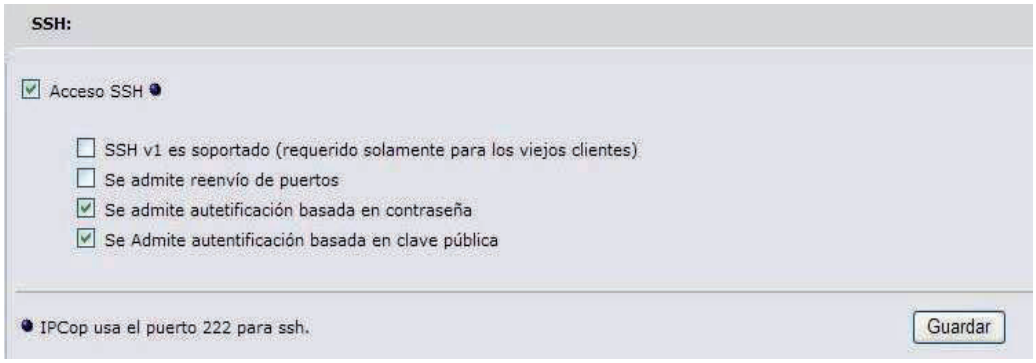


Fig. 2. 20 Acceso SSH

Una vez hecho esto, se puede ejecutar WinSCP, los datos requeridos son: IP de la interfaz verde, puerto usado por IPCop, usuario root y la contraseña que se estableció en la instalación.

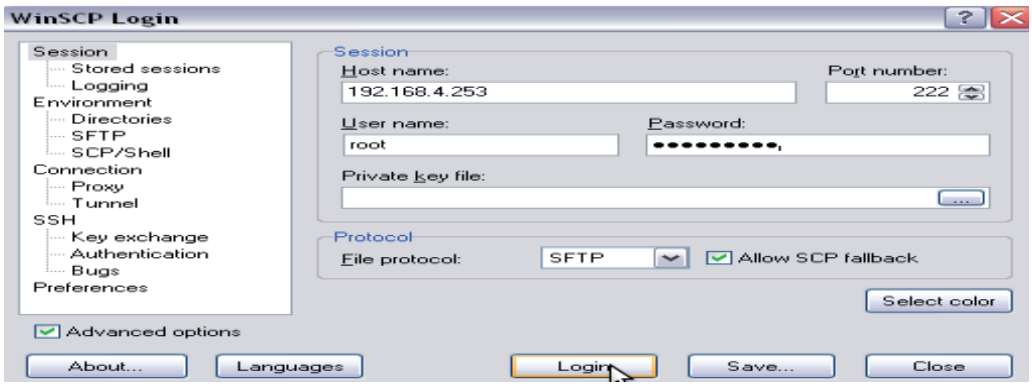


Fig. 2. 21 Conexión mediante WinSCP

Al abrir, la ventana del lado izquierdo mostrará las carpetas que hay en el equipo local, solo habrá que buscar el directorio donde se guardo la carpeta Addons; del lado derecho se encuentran las carpetas de sistema de IPCop, para pasar la carpeta Addons solo se arrastra del origen a la carpeta de root.

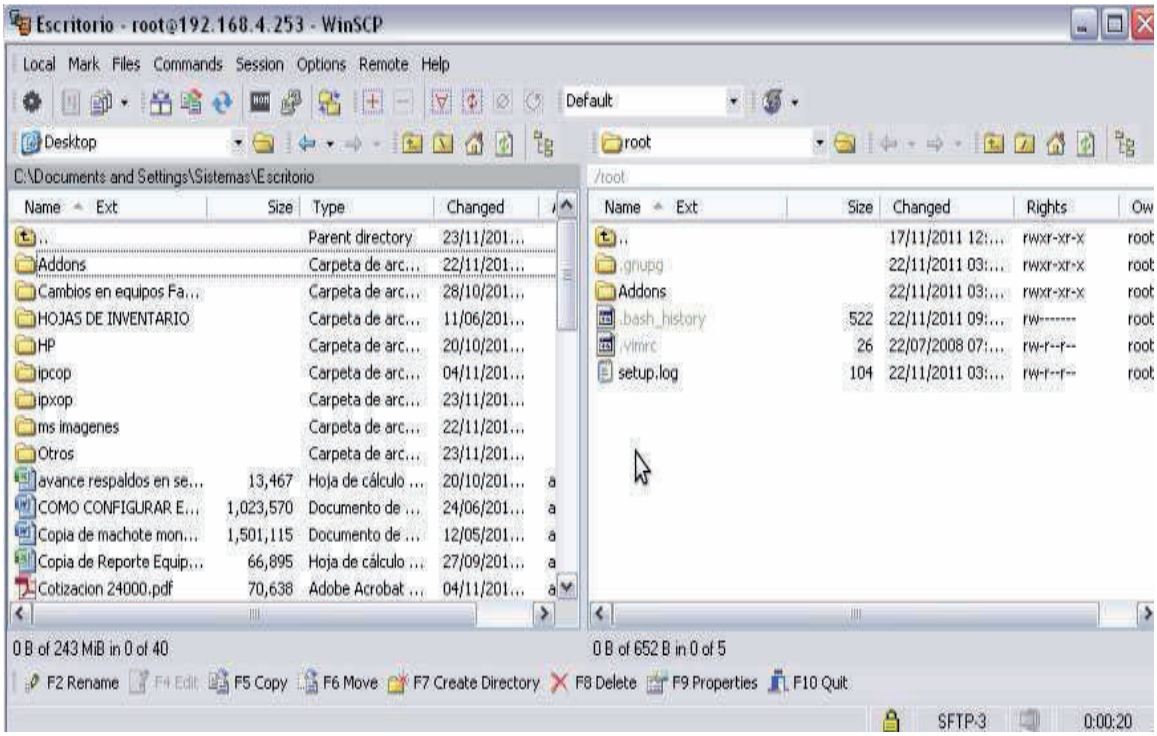


Fig. 2. 22 Transferencia de archivos usando WinSCP

Una vez creada la carpeta Addons en el directorio root, habrá que entrar a la consola de comandos mediante PuTTY, los datos proporcionados son la IP de la interfaz VERDE y el puerto.

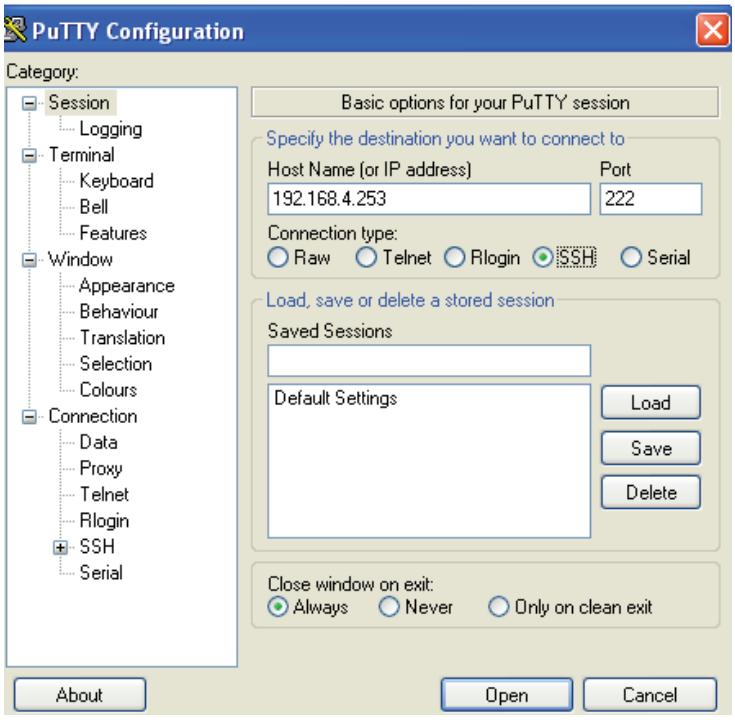


Fig. 2. 23 Conexión mediante PuTTY

Dentro de la consola, solicita la autenticación del usuario, para este caso, se proporciona el usuario root y la contraseña asignada. Con el comando *dir*, se puede comprobar que la carpeta Addons con todos los paquetes ya existe en el directorio.

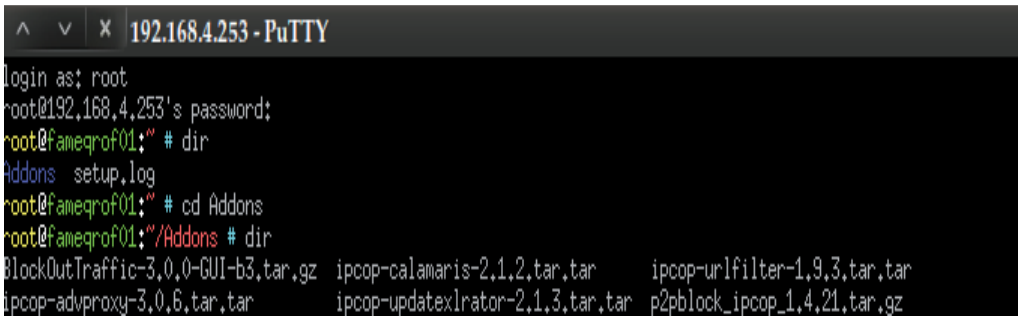


Fig. 2. 24 Consola IPCop

Para realizar la instalación de los paquetes, se usarán los comandos siguientes:

- *cd –Nombre del directorio-* Entrar a un directorio.
- *cd ..* Regresar al directorio anterior.
- *tar zxvf –Nombre del archivo a descomprimir-* Descomprimir archivos.
- *./install* Instalar el Add-on desde el directorio actual.
- *./setup* Instalar el Add-on BlockOutTraffic

Primero se descomprimen los archivos.

Fig. 2. 25 Descomprimir Add-on

Posteriormente, habrá que ingresar a los directorios marcados en color azul para ejecutar la instalación:

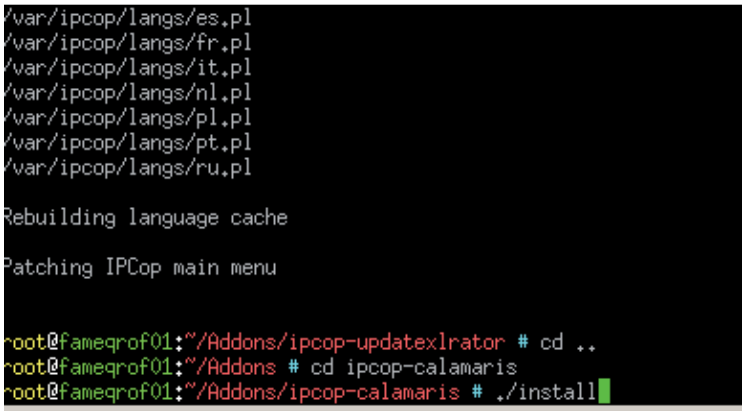


Fig. 2. 26 Instalación de Add-on

Hasta este momento, ya están instalados IPCop y los Add-on; ahora es posible tener acceso a listas negras de páginas WEB maliciosas, crear listas blancas, bloquear usuarios, poner mensajes, crear grupos para acceso limitado o abierto.

Cabe destacar que debido a que los Add-on no están oficialmente soportados, no es inusual que una actualización haga desaparecer algún Add-on o algún punto de menú del mismo, por lo que se debe prestar especial atención a las actualizaciones.

2.4 ADMINISTRACIÓN

En esta sección se muestra como se administra IPCop. La página de administración permite navegar entre los siguientes menús:

- Sistema.
- Estado.
- Red.
- Servicios.
- Firewall.
- VPNs.
- Logs.

De los cuales se describe el uso y configuración.

2.4.1 Sistema

Este grupo de páginas está diseñado para ayudar a administrar y controlar el acceso a IPCop. A continuación se describe cada uno de los menús.

2.4.1.1 Inicio

La página de inicio varía dependiendo de la configuración que se eligió para la interfaz ROJA. Su función principal es mostrar información básica del tipo de conexión, el tiempo que ha estado conectado desde el último reinicio, dirección IP, así como el número de usuarios logueados y el icono que es posible encontrar en todas las páginas que envía directo al sitio de ayuda de IPCop.

Fig. 2. 27 Pantalla de inicio acceso Web

2.4.1.2 Actualizaciones

Esta página se divide en 2 secciones:

El primer cuadro muestra la lista de actualizaciones disponibles para su descarga y se puede seleccionar el tipo de Kernel para guardar las actualizaciones en caso de que el espacio en disco sea bajo.

El segundo cuadro muestra la lista de actualizaciones que han sido instaladas.

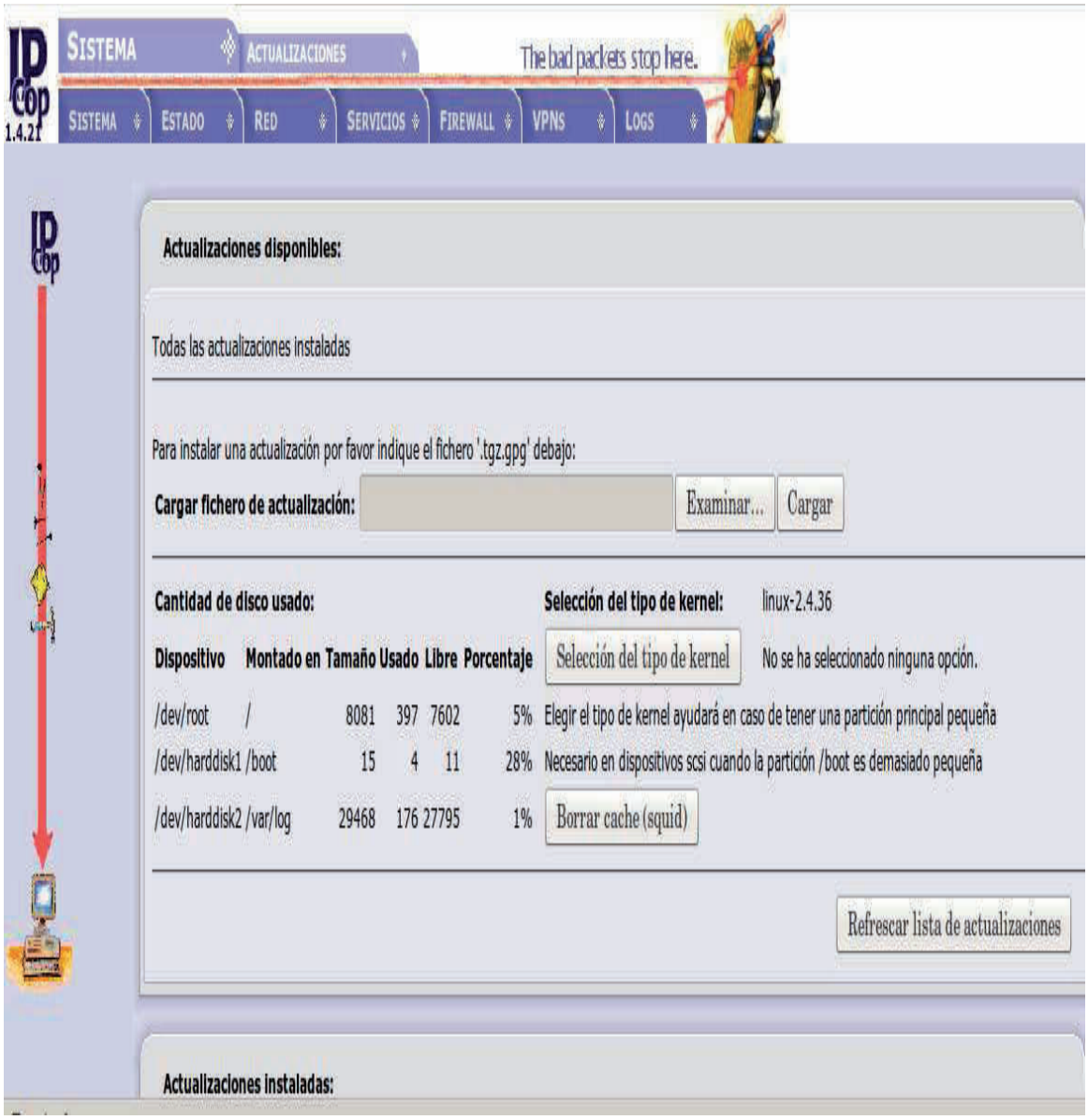


Fig. 2. 28 Actualizaciones disponibles e instaladas

Mientras esté conectado a Internet, IPCop automáticamente detectará las actualizaciones, es importante liberar el espacio en disco, para este propósito esta el botón Borrar cache (Squid).

2.4.1.3 Contraseñas

Esta página permite cambiar las contraseñas de Admin y/o el usuario Dial, para la activación de este último solo basta con ingresar una contraseña, este usuario solo tendrá acceso a la página principal para conectar o desconectar el Internet y no podrá modificar la configuración del Firewall.

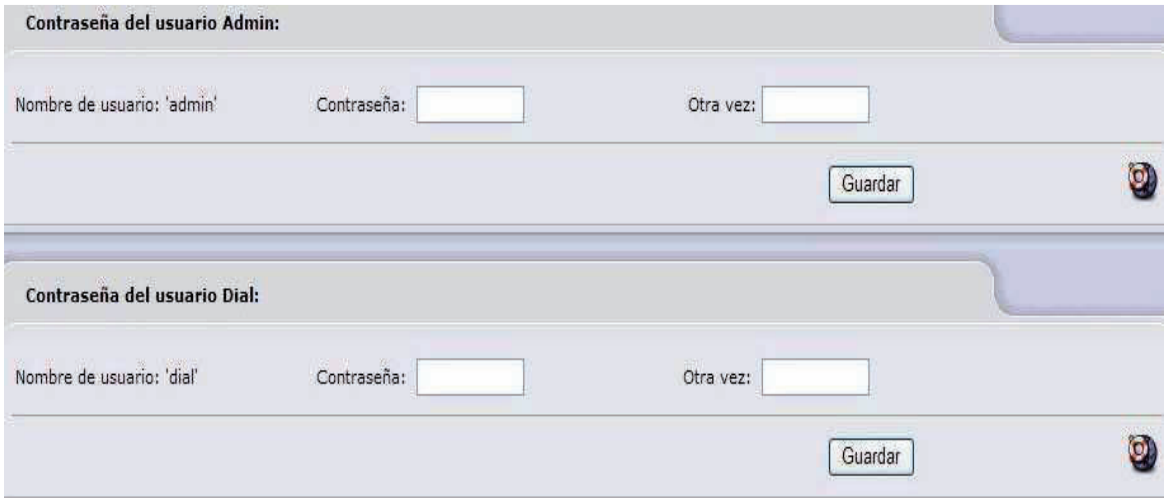


Fig. 2. 29 Administración de contraseñas

2.4.1.4 Acceso SSH

Si se desea dar acceso a conexiones remotas SSH a través de la interfaz VERDE, se habilita el checkbox.

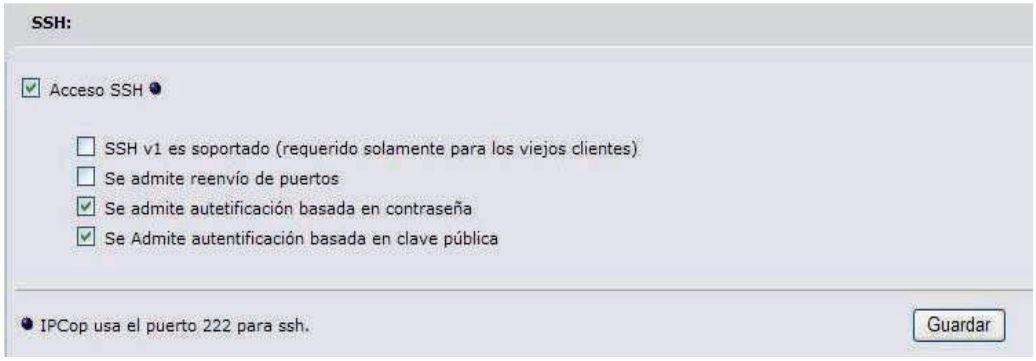


Fig. 2. 30 Acceso SSH

2.4.1.5 Ajustes GUI

Esta página rige la forma en que aparecerán las páginas del sitio de IPCop. Aunque también permite deshacer los cambios al presionar el botón Valores predeterminados.

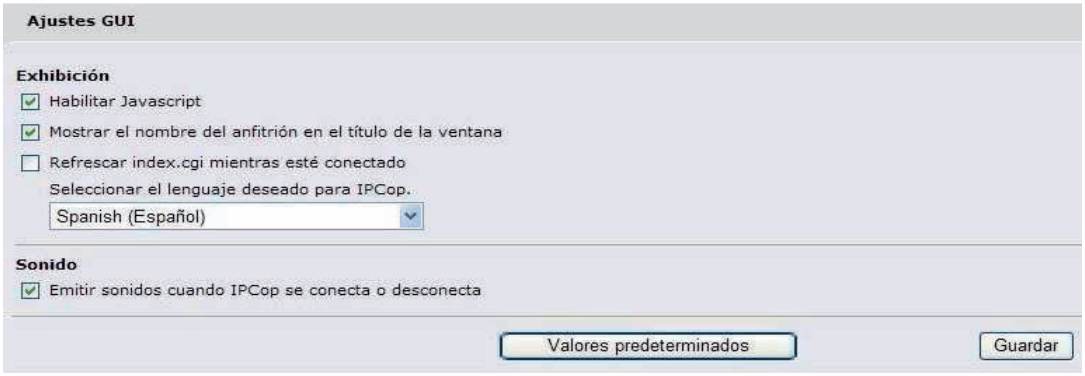


Fig. 2. 31 Ajustes GUI

2.4.1.6 Respaldar

IPCop permite hacer copias de respaldo en diferentes medios, desde un floppy hasta un dispositivo USB, éstos, son enviados a un archivo .dat. Es necesario conocer la contraseña del usuario 'backup' que se definió al inicio.

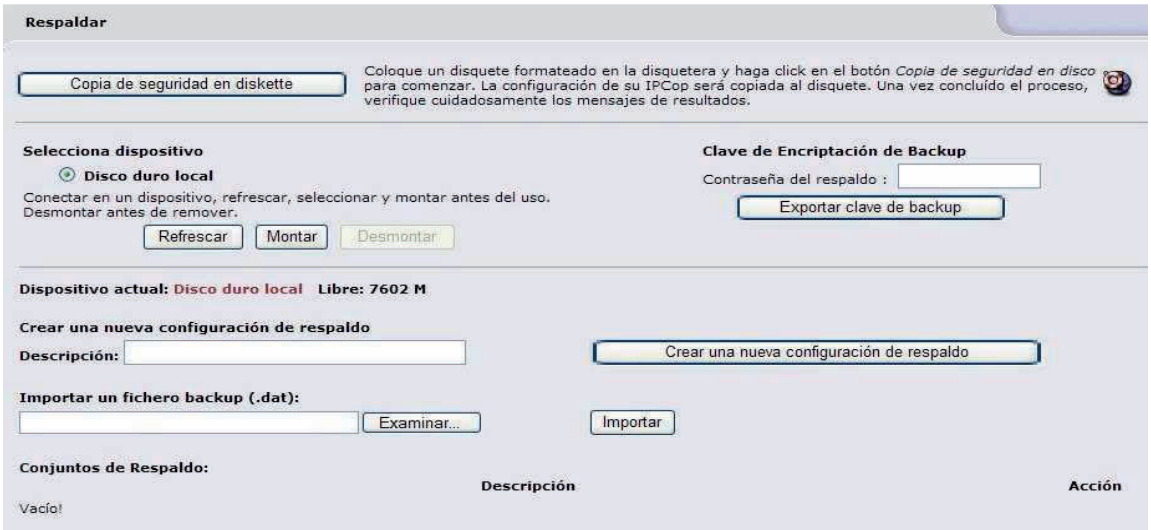


Fig. 2. 32 Respaldar

2.4.1.7 Apagar

Esta página permite no solo apagar o reiniciar el equipo, sino también, en caso de ser necesario programar estas acciones.

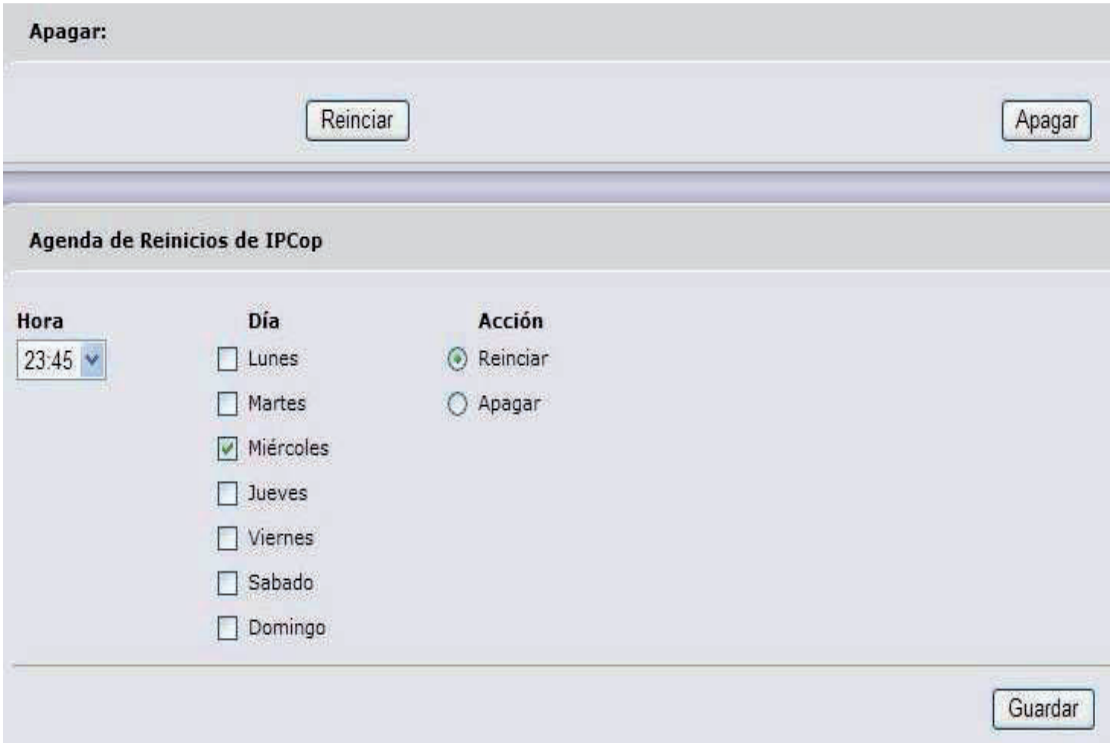


Fig. 2. 33 Programar reinicios o apagar

2.4.2 Estado

Esta ficha presenta una lista completa de información sobre el estado actual de IPCop.

2.4.2.1 Estado del sistema

La página muestra información tal como los servicios que están corriendo, el uso de la memoria, el total de espacio en disco duro e información del Kernel.

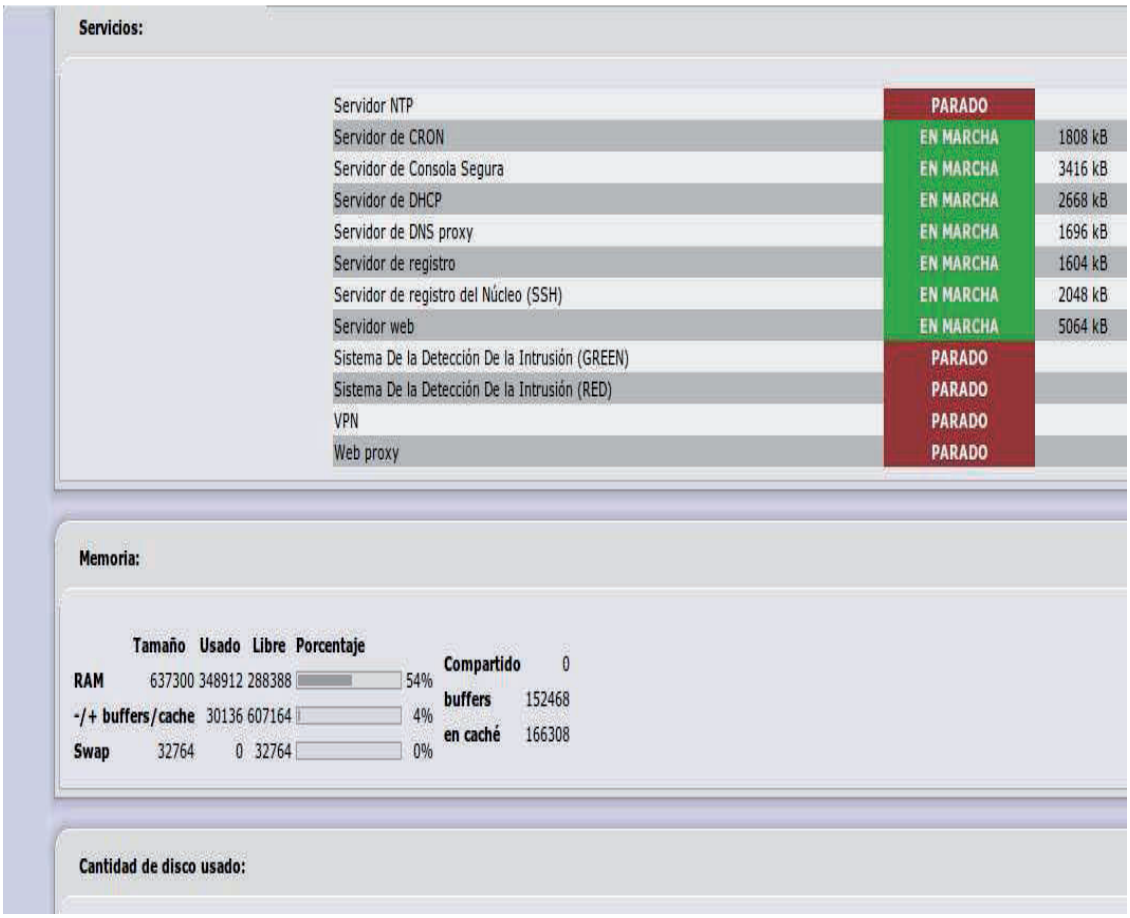


Fig. 2. 34 Estado del sistema

2.4.2.2 Estado de la red

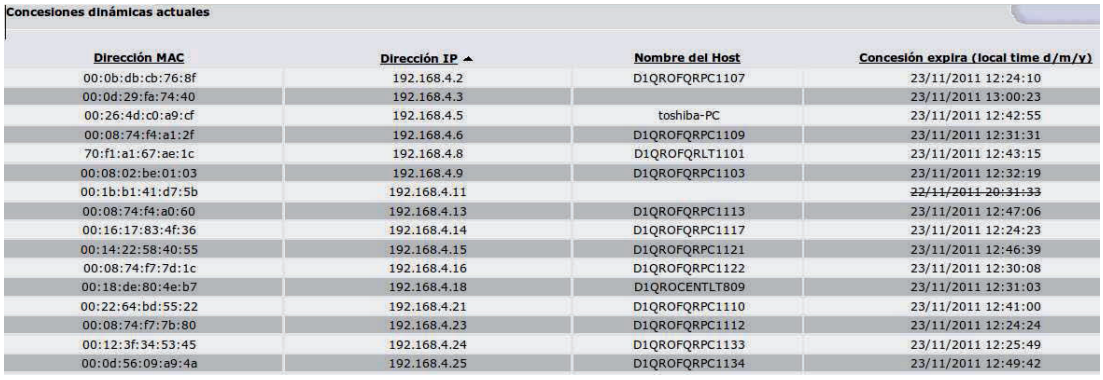
Esta pantalla muestra la información de todas las tarjetas de red.

Interfaces:

```
eth0      Link encap:Ethernet  HWaddr 00:60:08:A6:DE:54
          inet addr:192.168.4.253  Bcast:192.168.4.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2929980 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3868721 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:490614611 (467.8 MB)  TX bytes:277054905 (264.2 MB)
          Interrupt:5 Base address:0x1000

eth1      Link encap:Ethernet  HWaddr 00:0C:76:05:53:4F
          inet addr:1.1.1.1  Bcast:1.1.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING  MTU:1500  Metric:1
          RX packets:4020956 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2672696 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:340417148 (324.6 MB)  TX bytes:475857068 (453.8 MB)
          Interrupt:5 Base address:0x1040 Memory:fc500000-fc500038

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8053 (7.8 KB)  TX bytes:8053 (7.8 KB)

ppp0      Link encap:Point-to-Point Protocol
          inet addr:187.194.33.217  P-t-P:200.38.193.226  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1492  Metric:1
```

Fig. 2. 35 Estado de la red

La siguiente pantalla muestra el contenido del directorio */var/state/dhcp/dhcp.leases* mientras el DHCP este activo, enlista las direcciones IP asignadas a los equipos conectados a la red, así como su MAC ADDRESS y las fechas en que expiran las concesiones.



Concesiones dinámicas actuales

Dirección MAC	Dirección IP ▲	Nombre del Host	Concesión expira (local time d/m/y)
00:0b:db:cb:76:8f	192.168.4.2	D1QROFQRPC1107	23/11/2011 12:24:10
00:0d:29:fa:74:40	192.168.4.3		23/11/2011 13:00:23
00:26:4d:c0:a9:cf	192.168.4.5	toshiba-PC	23/11/2011 12:42:55
00:08:74:f4:a1:2f	192.168.4.6	D1QROFQRPC1109	23/11/2011 12:31:31
70:f1:a1:67:ae:1c	192.168.4.8	D1QROFQRLT1101	23/11/2011 12:43:15
00:08:02:be:01:03	192.168.4.9	D1QROFQRPC1103	23/11/2011 12:32:19
00:1b:b1:41:d7:5b	192.168.4.11		~~22/11/2011 20:31:33~~
00:08:74:f4:a0:60	192.168.4.13	D1QROFQRPC1113	23/11/2011 12:47:06
00:16:17:83:4f:36	192.168.4.14	D1QROFQRPC1117	23/11/2011 12:24:23
00:14:22:58:40:55	192.168.4.15	D1QROFQRPC1121	23/11/2011 12:46:39
00:08:74:f7:7d:1c	192.168.4.16	D1QROFQRPC1122	23/11/2011 12:30:08
00:18:de:80:4e:b7	192.168.4.18	D1QROCENTLT809	23/11/2011 12:31:03
00:22:64:bd:55:22	192.168.4.21	D1QROFQRPC1110	23/11/2011 12:41:00
00:08:74:f7:7b:80	192.168.4.23	D1QROFQRPC1112	23/11/2011 12:24:24
00:12:3f:34:53:45	192.168.4.24	D1QROFQRPC1133	23/11/2011 12:25:49
00:0d:56:09:a9:4a	192.168.4.25	D1QROFQRPC1134	23/11/2011 12:49:42

Fig. 2. 36 Concesiones DHCP

Las últimas secciones muestran la tabla de ruteo y el contenido de la tabla de ARP (Address Resolution Protocol).

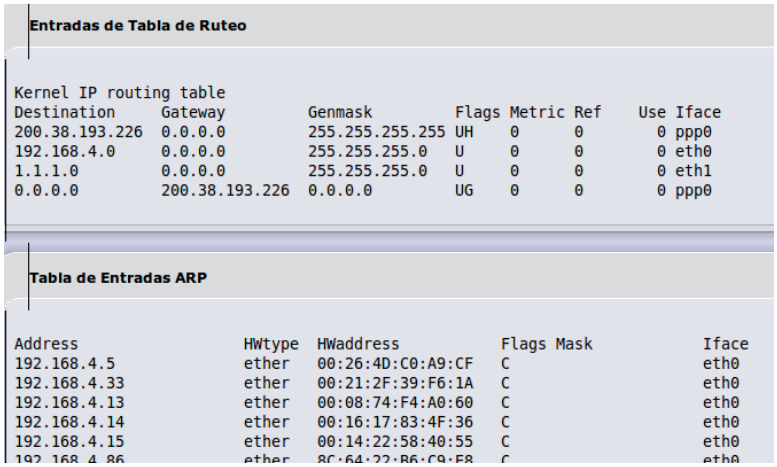


Fig. 2. 37 Entradas de Tabla de ruteo y ARP

2.4.2.3 Gráficos del sistema

En esta página se encuentran las representaciones gráficas de uso de los recursos del equipo, el tráfico de entrada/salida y acceso al proxy de IPCop por periodos de días hasta años. Si no se mostraran habrá que ejecutar le comando *'makegraphs'* desde la consola.

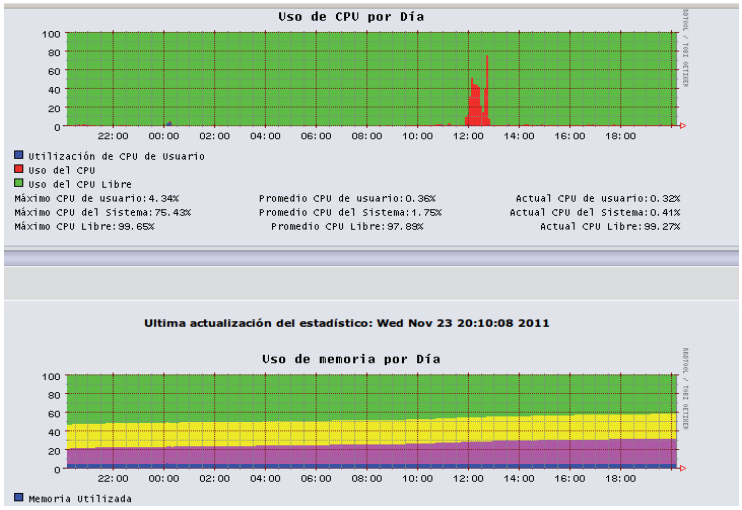


Fig. 2. 38 Gráficos del sistema

2.4.2.4 Conexiones

La información que se muestra en la página, hace referencia a los puertos de origen y destino de las direcciones IP de la red, así como en el estado de la conexión, solo los paquetes de conformidad se permiten a través del firewall. Las ventanas muestran las conexiones de IPtables y están codificadas por colores en función de su ubicación en la red, la leyenda del código de colores se muestra en la parte superior de la página.

Rastreo de Conexión de IPTables

Leyenda : LAN | INTERNET | DMZ | Inalambrica | IPCop | VPN

Protocolo	Caducidad (Segundos)	Conexión Estado	Original IP:Puerto de Origen	Original IP:Puerto de destino	Esperado IP:Puerto de Origen	Esperado IP:Puerto de destino	Marcado	Uso
Todos/as		Todos/as	*.*.*.*	*.*.*.*	Clase en Orden Ascendente:	orgsip	Todos/as	!
udp (17)	24		187.194.33.217 :45846	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :45846		1
udp (17)	1		187.194.33.217 :15136	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :15136		1
udp (17)	24		187.194.33.217 :31433	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :31433		1
udp (17)	14		187.194.33.217 :6033	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :6033		1
udp (17)	11		187.194.33.217 :23059	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :23059		1
udp (17)	5		187.194.33.217 :61697	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :61697		1
udp (17)	1		187.194.33.217 :33215	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :33215		1
udp (17)	14		187.194.33.217 :17700	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :17700		1
tcp (6)	88	TIME_WAIT	187.194.33.217 :32959	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :32959	[ASSURED]	1
udp (17)	14		187.194.33.217 :21815	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :21815		1
udp (17)	11		187.194.33.217 :35133	200.23.242.226 :53	200.23.242.226 :53	187.194.33.217 :35133		1
igmp (2)	518		192.168.1.254 :	224.0.0.1 :	224.0.0.1 :	192.168.1.254 :	[UNREPLIED]	
udp (17)	9		192.168.4.2 :137	192.168.4.255 :137	192.168.4.255 :137	192.168.4.2 :137	[UNREPLIED]	1
tcp (6)	402789	ESTABLISHED	192.168.4.2 :4741	201.249.110.245 :42844	201.249.110.245 :42844	187.194.33.217 :4741	[ASSURED]	1
udp (17)	5		192.168.4.2 :64780	192.168.4.253 :53	192.168.4.253 :53	192.168.4.2 :64780		1
udp (17)	5		192.168.4.2 :55710	192.168.4.253 :53	192.168.4.253 :53	192.168.4.2 :55710		1
tcp (6)	431914	ESTABLISHED	192.168.4.5 :49476	74.125.224.200 :80	74.125.224.200 :80	187.194.33.217 :49476	[ASSURED]	1

Fig. 2. 39 Rastreo de conexión de IPTables

2.4.3 Red

En esta sección se encuentran las opciones para el marcado y configuración hacia una conexión de Internet.

2.4.3.1 Marcado

La página se divide en 5 secciones y solo se aplica si el acceso a Internet es a través de un módem análogo, un dispositivo ISDN o una conexión DSL. En cada sección se indica la forma en que la tarjeta roja buscará conectarse a Internet.

Fig. 2. 40 Marcado

Para realizar modificaciones, es necesario desconectar los servicios desde la página de inicio.

2.4.4 Servicios

2.4.4.1 Advanced proxy

Habilitar en Green, permite al servidor Proxy escuchar las peticiones de los clientes en esta interfaz. El puerto Proxy es por el que escuchará las peticiones de los clientes. El valor por defecto es 800, en este caso se colocará el 8889 para diferenciarlo; en modo transparente, las solicitudes del puerto 80(HTTP) son automáticamente redirigidas hacia este puerto.

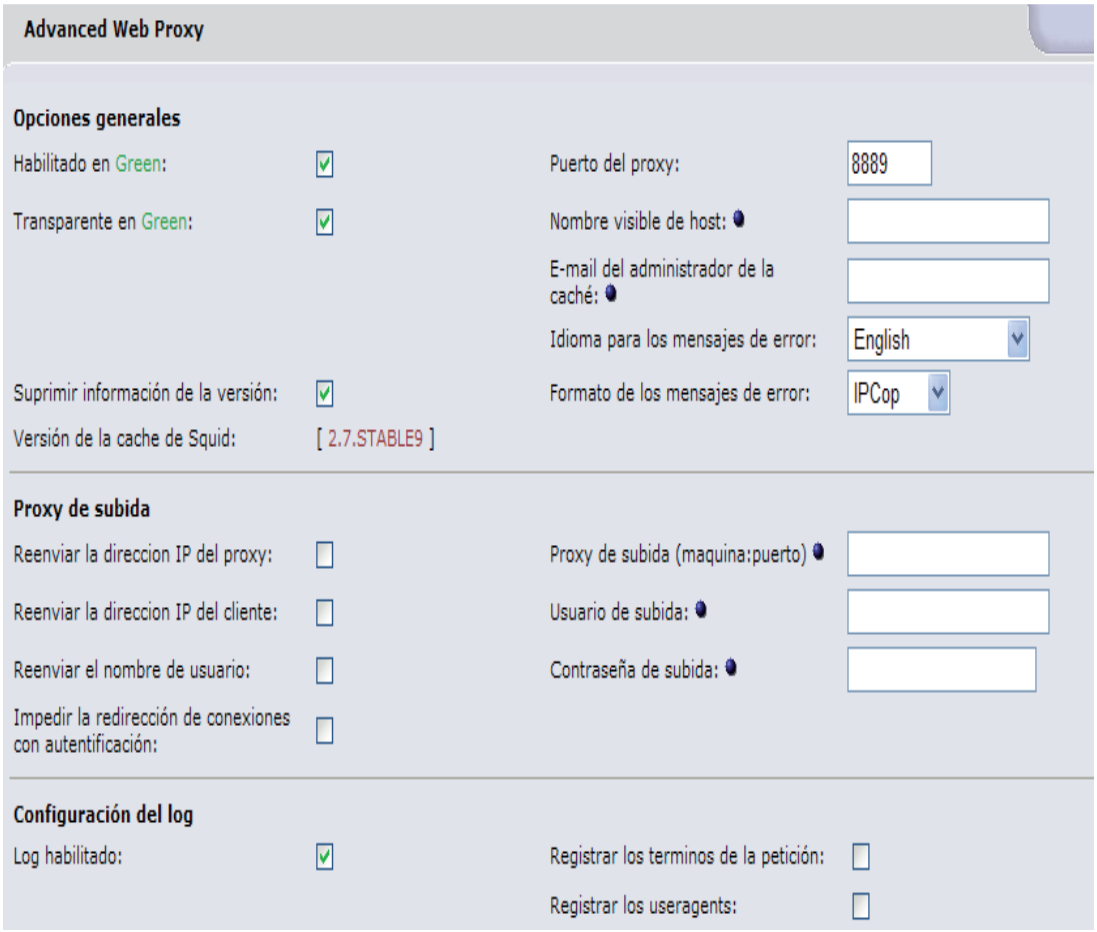


Fig. 2. 41 Configuración de ADV Proxy

Si el Proxy se configura en modo transparente no se requiere ningún tipo de configuración de Proxy en las estaciones de trabajo de la red local, se denomina transparente porque el cliente en realidad no sabe que lo está usando, es transparente para él.

En cambio, si el Proxy se configura en modo normal el usuario deberá configurar su navegador y todos los programas que accedan a Internet con la dirección IP de la interfaz Verde. Habilitar esta opción permite un mayor control de las actividades del usuario.

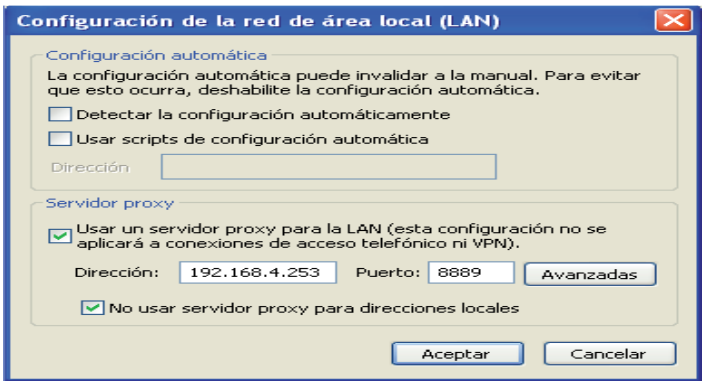


Fig. 2. 42 Configuración del Proxy en I. Explorer

Dentro de la misma sección, es posible elegir la cantidad de espacio en disco que se puede utilizar para almacenar en caché las páginas web; también, agrega puertos estándar para el acceso a sitios web, si alguno no estuviera basta con agregarlo y guardarlo.

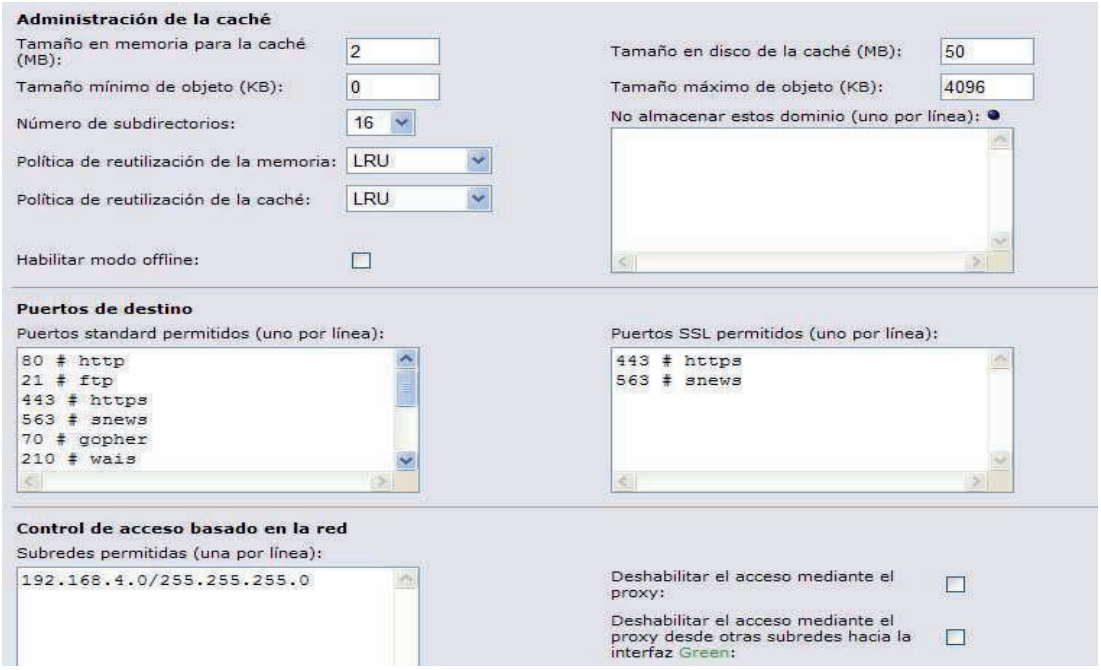


Fig. 2. 43 Administración de caché y puertos

Esta página también permite restringir los accesos por tiempo, tamaños máximos de descarga, así como definir límites dependiendo del tipo de archivo.

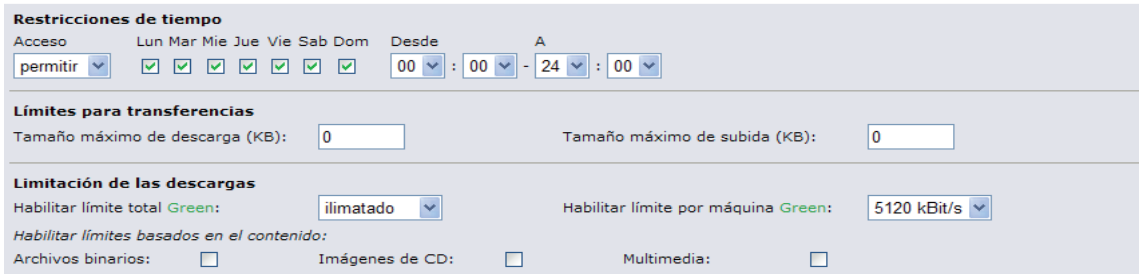


Fig. 2. 44 Restricciones de tiempo

2.4.4.2 Filtro de URL

Entre las múltiples categorías que en la primera sección se muestran para bloquear, la Fig. 2.45 indica las que no serán permitidas.

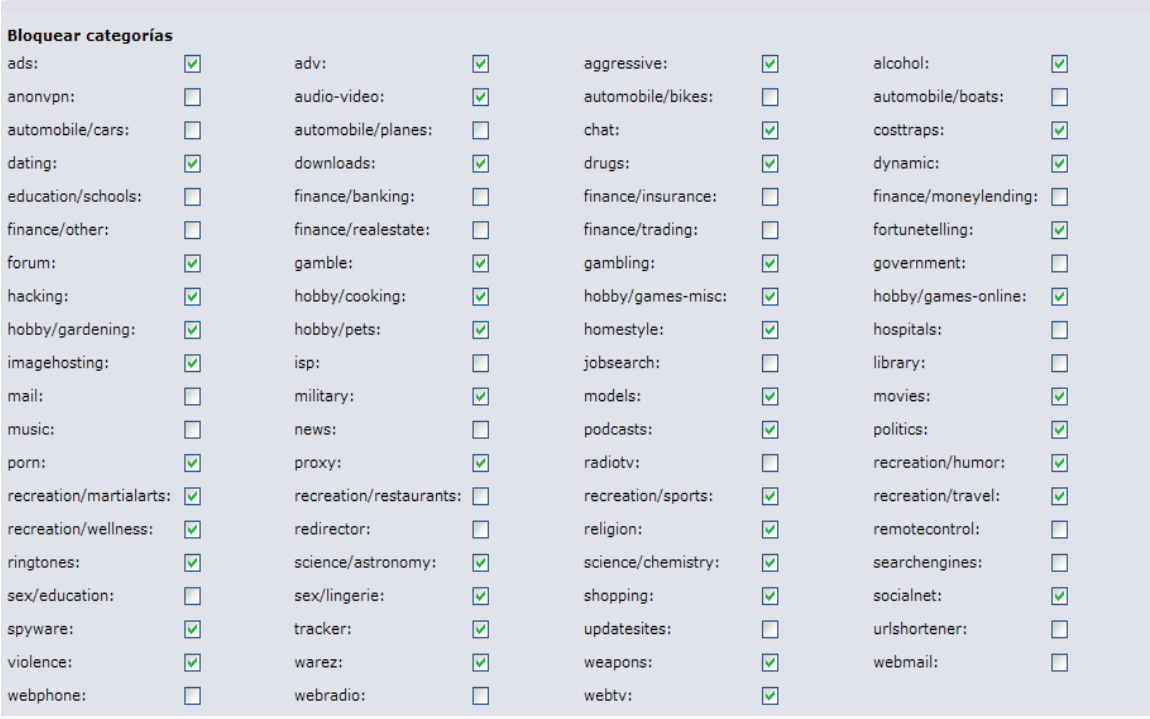


Fig. 2. 45 Bloqueo de categorías con Filtro de URL

Al iniciar se muestran pocas categorías, para corregir esto, solo bastará con actualizar, cuando ésta finaliza, se muestran el resto de categorías por bloquear.

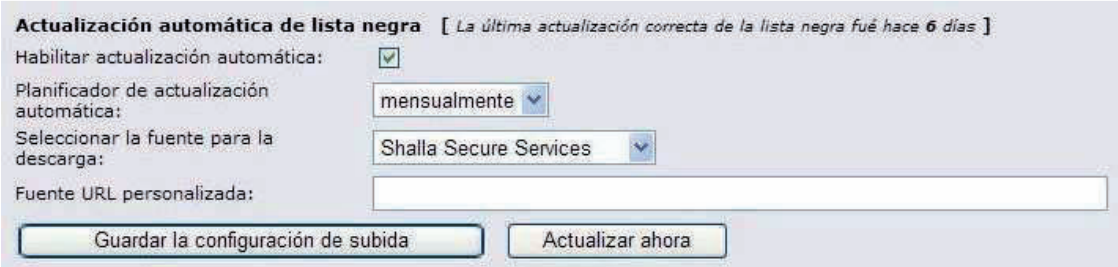


Fig. 2. 46 Actualización de lista negra

En el siguiente apartado es posible bloquear o permitir dominios, así como colocar la o las direcciones IP que tengan acceso a todos los sitios y controlar el tiempo de acceso.

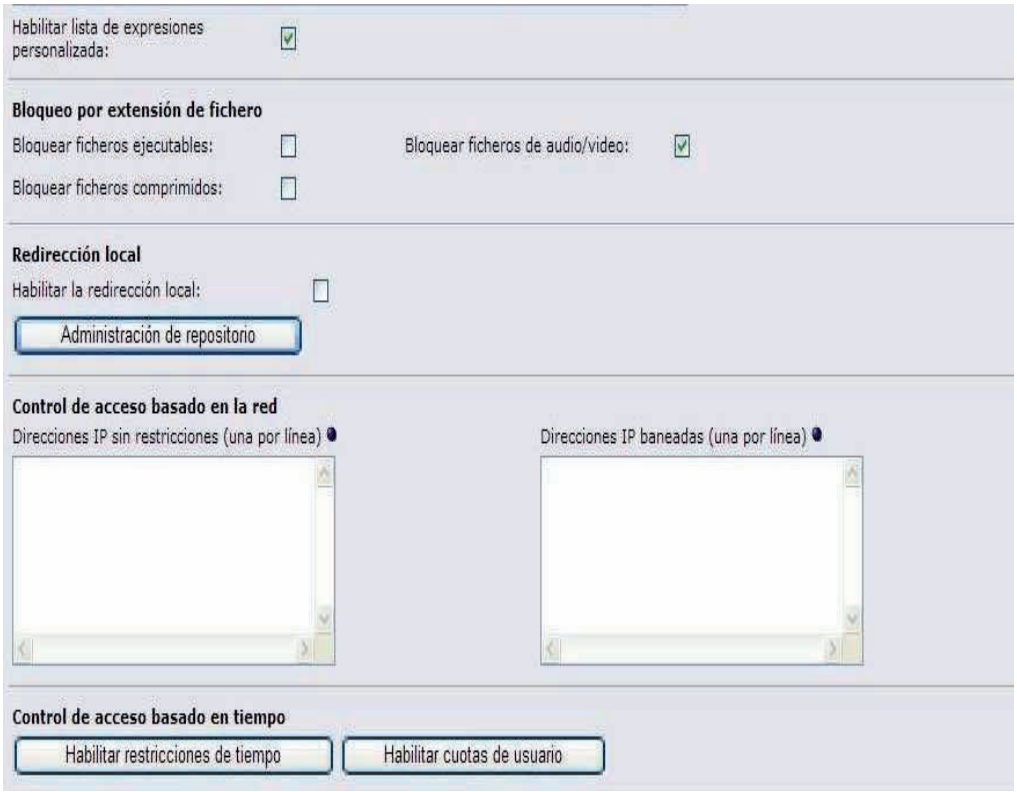


Fig. 2. 47 Bloqueo de archivos según su tipo

Se puede modificar la página que verán los usuarios cuando intenten ingresar a un sitio que no está permitido, la configuración permite redirigir a una URL, o configurar los datos que indicarán que el acceso no está permitido.

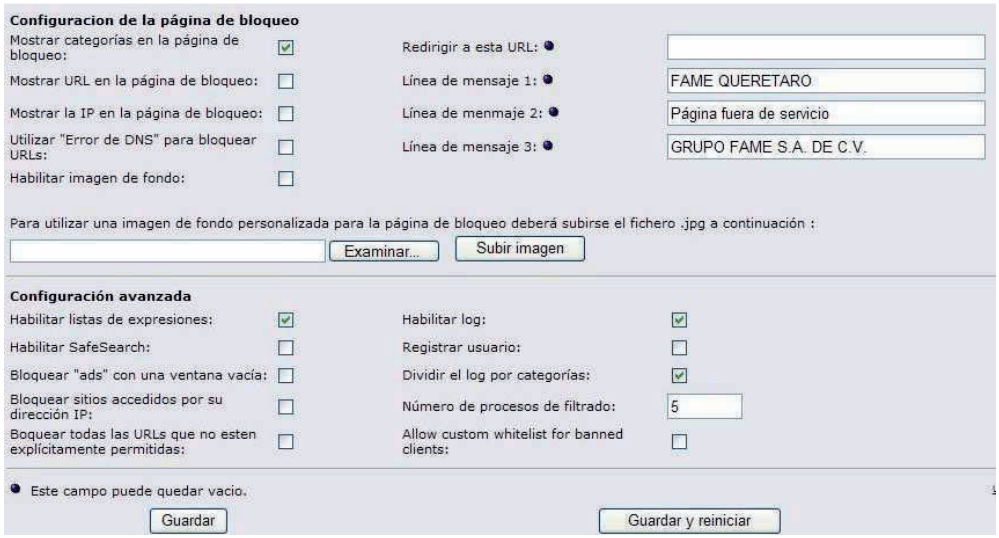


Fig. 2. 48 Configuración de pantalla de bloqueo

De esta forma cuando los usuarios traten de ingresar a sitios que fueron restringidos por el Administrador, en los navegadores aparecerá el mensaje.

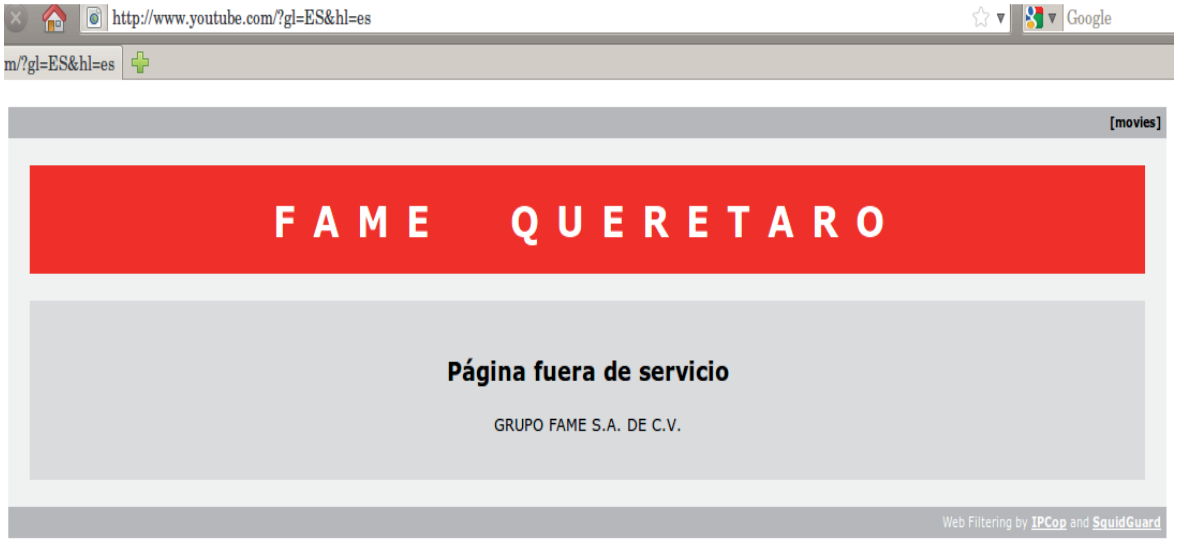


Fig. 2. 49 Pantalla de bloqueo

Dentro de esta categoría, también es posible crear copias de seguridad de la configuración del filtro de URL por si llegara a ser necesario restaurar.

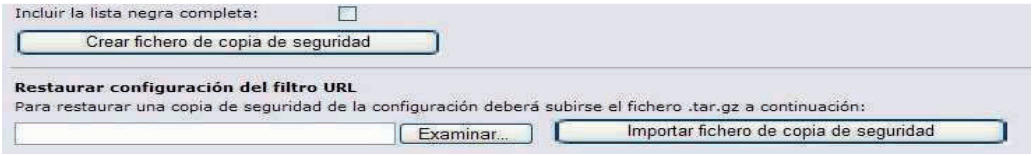


Fig. 2. 50 Copias de seguridad

Cuando se termina la configuración, es necesario habilitarlo en Advanced Proxy.

Fig. 2. 51 Habilitar Filtro de URL

2.4.4.3 Acelerador de actualización

La configuración será la siguiente:

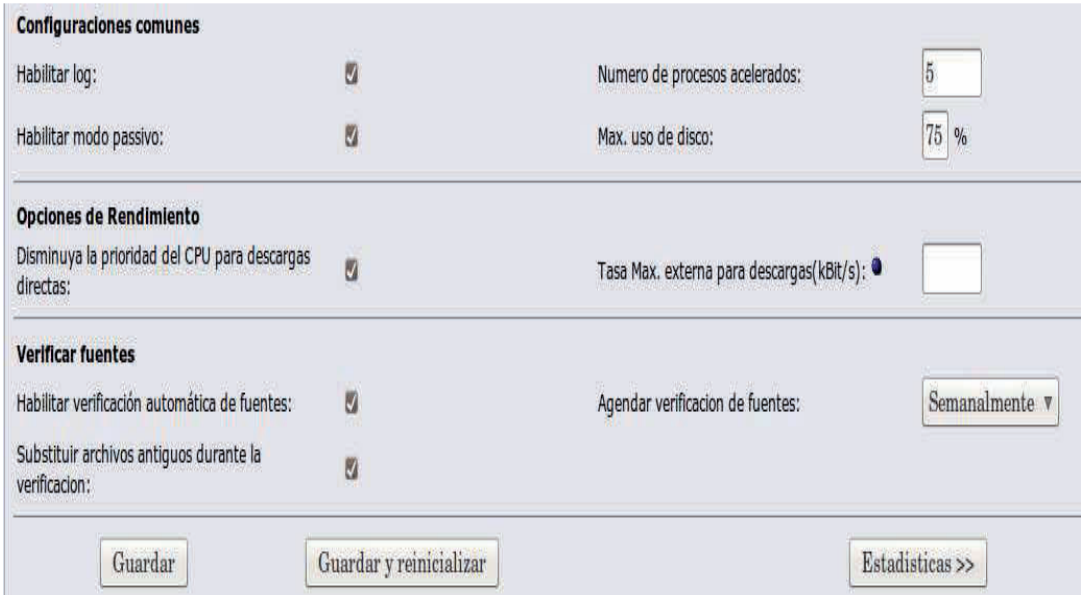


Fig. 2. 52 Acelerador de actualización

Para trabajar con él se debe acceder a Advanced Proxy y habilitarlo para poder ponerlo en marcha.

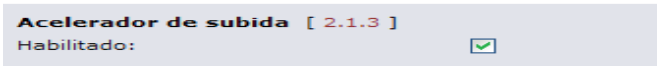


Fig. 2. 53 Acelerador de subida

2.4.4.4 Servidor DHCP

Esta opción se activa si se desea obtener la configuración de la red automáticamente, de esta forma, cuando una computadora o dispositivo se conecte a la red local, le será asignada una dirección IP y los DNS proporcionadas por IPCop, se puede asignar el rango de las IP así como el tiempo de concesión para cada dirección.

Fig. 2. 54 Servidor de DHCP

Si el DHCP se encuentra activo, se muestra la lista de las concesiones contenidas en el archivo */var/state/dhcp/dhcp.leases*; se pueden asignar concesiones fijas cuando se requiera que un equipo se conecte con la dirección IP indicada mediante su MAC, esta operación se activa desde el botón crear concesiones fijas, que se encuentra en la parte inferior de la página.

Fig. 2. 55 Crear concesiones fijas

2.4.4.5 Servidor de horario

IPCop puede ser configurado para obtener la hora de servidor de horas a través de internet, incluso puede proporcionar el tiempo a otros equipos en la red local. En su caso, es posible configurar la hora manualmente.

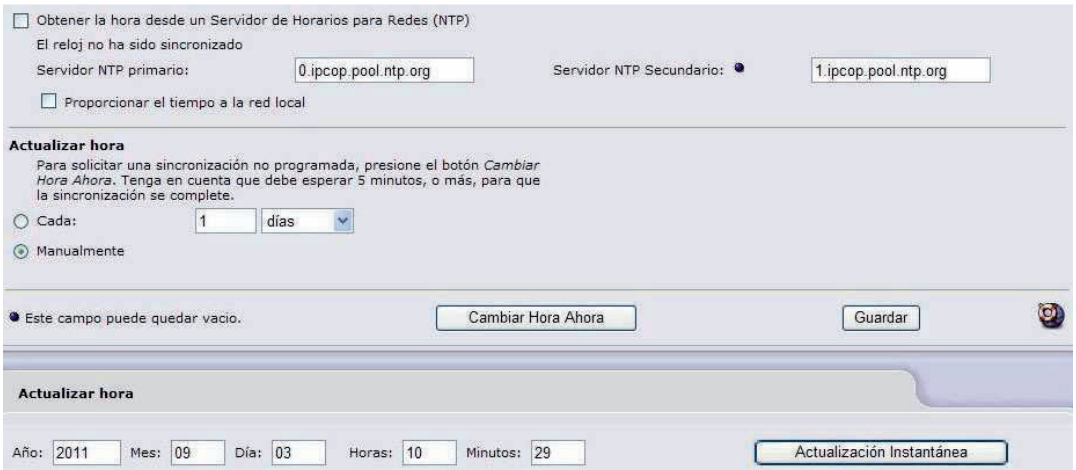


Fig. 2. 56 Servidor de horario

2.4.4.6 P2PBlock

Este Add-on usa IPtables, cadenas de búsqueda, layer7-filter e ipp2p-filter para bloquear todo el tráfico P2P (Peer-to-Peer). Su funcionamiento solo requiere que se activen los checkbox y aplicar la configuración.

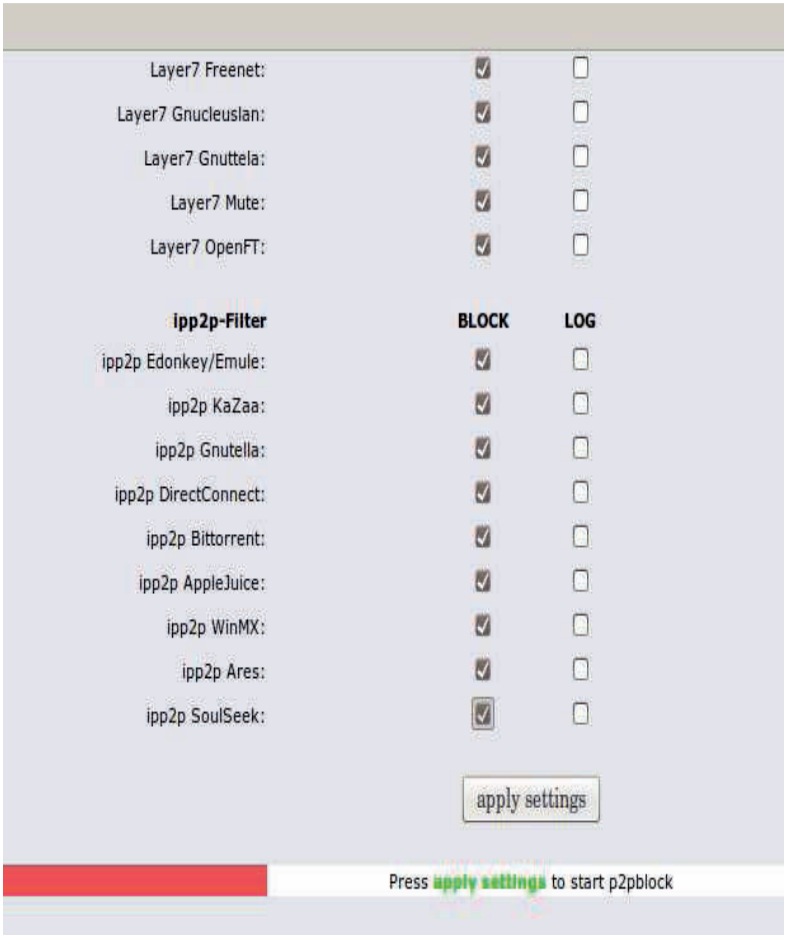


Fig. 2. 57 Bloqueo P2P

Las conexiones P2P que se hayan establecido hasta el momento seguirán funcionando, pero en el siguiente intento ya no podrán iniciar la descarga.

2.4.4.7 Control de tráfico

Permite priorizar el tráfico de IP que se mueve a través del Firewall, esto se logra mediante WonderShaper, éste fue diseñado para minimizar la latencia de ping. IPCop prioriza el tráfico de la forma que se configure en esta sección, dividiéndolo en bajo, medio o alto.

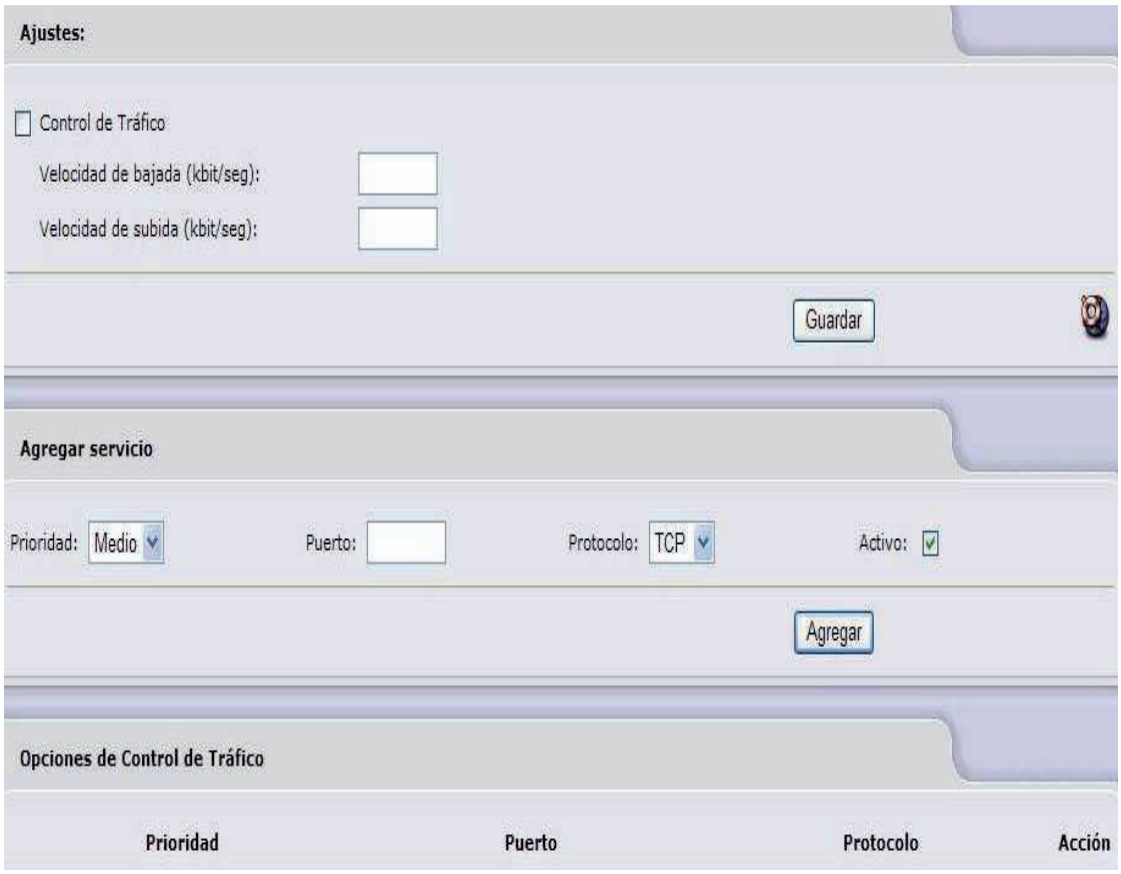


Fig. 2. 58 Control de tráfico

2.4.4.8 Detección de intrusión

IPCop contiene un sistema de detección de intrusiones de gran alcance, Snort, que analiza el contenido de los paquetes recibidos por el firewall y la búsqueda de actividades maliciosas. Snort es un sistema pasivo que requiere que el usuario configure las opciones para controlar los registros e interpretar la información. Para volverlo un sistema activo, es necesario usar *snort_inline* o el Add-on *guardian*.

Es importante tener en cuenta que Snort consume recursos en memoria, de hasta 80MB por cada interfaz dependiendo del conjunto de reglas utilizadas.

Fig. 2. 59 Detección de intrusión

2.4.5 BlockOutTraffic

Su activación bloqueará todo lo que no salga por los puertos que estén configurados; sin embargo, se tendrá mayor control al especificar los servicios y equipos que tendrán acceso. Al ingresar a *Firewall/Bloquear tráfico de salida* por primera vez, aparecerá un mensaje de error indicando que la configuración actual no es válida. Así que habrá que ajustar la configuración.

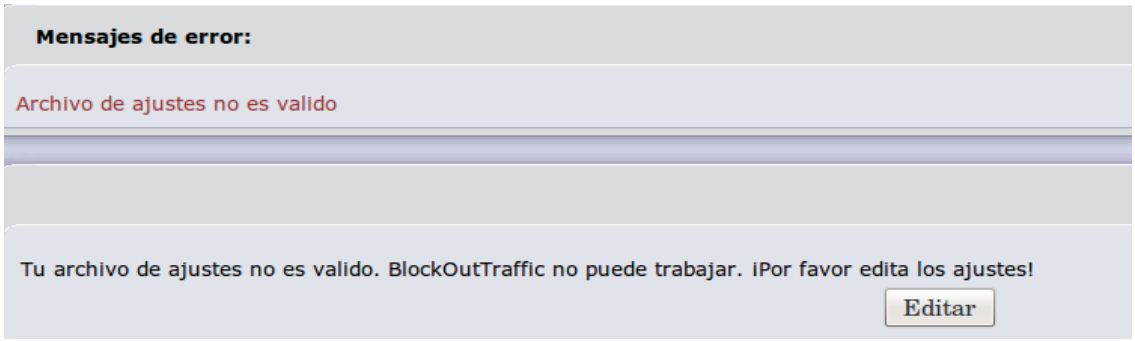


Fig. 2. 60 BlockOutTraffic

Los datos que son requeridos para este propósito son el puerto HTTPS y la MAC del equipo que se usará para administrarlo, ya que una vez activo y si no se crea la regla, solo este equipo tendrá acceso a la página de administración.

Fig. 2. 61 Ajustes BOT

Si estos datos no se dieran de alta y se activa el BOT, no se podrá ingresar a la página de administración, si eso pasará, mediante la consola es posible usar los siguientes comandos:

/etc/rc.d/rc.firewall.local { start | stop | reload }

Antes de crear las reglas, habrá que ingresar a *Firewall/Configuración Avanzada del BOT* a dar de alta los siguientes parámetros.

Opciones de Servicios. El primer paso es dar de alta los servicios que permitirán el tráfico a través de Firewall, en la página debe estar seleccionada la opción correcta.

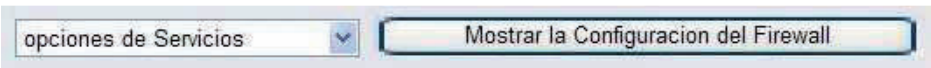


Fig. 2. 62 Opciones de servicios

En el siguiente apartardo es posible ingresar datos para dar de alta servicios personalizados, se debe indicar el nombre, puerto y protocolo por cada servicio que se necesite.

Fig. 2. 63 Agregar servicios

Los Servicios, puertos y protocolos son indicados a continuación:

Tabla 2. 1 Servicios a dar de alta

NOMBRE DE SERVICIO	PUERTO	PROTOCOLO
IPCop HTTPS	445	TCP
IPCop Proxy	8889	TCP
IPCop SSH	222	TCP
Ping		ICMP
Correo FAME	2525	TCP
WebMail FAME	2096	TCP
WebServices MP	8080	TCP
Amigo Nuevo	8084	TCP

Parámetros de Agrupación: El siguiente paso es dar de alta los grupos de servicios, para esto se cambia la opción a *Parámetros de Agrupación.*

Fig. 2. 64 Parámetros de agrupación

En esta sección se indicará el nombre del servicio de grupo, en caso de ser uno nuevo, o se seleccionará alguno si ya estuviera creado para dar de alta los servicios.

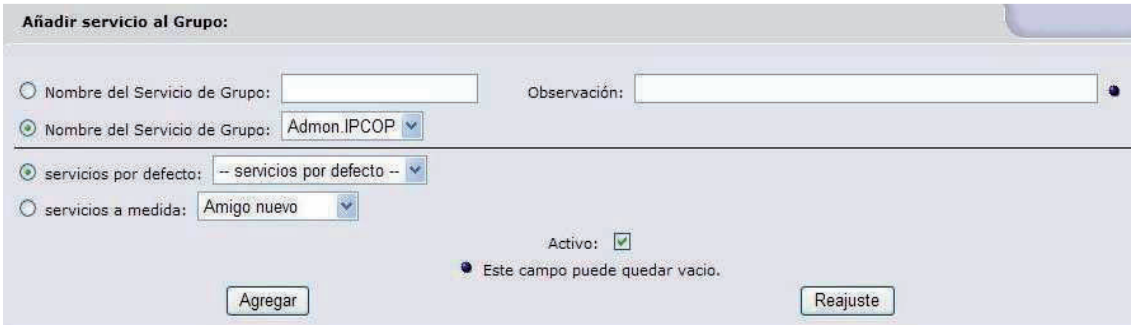


Fig. 2. 65 Añadir servicio al grupo

Los Grupos de Servicios serán los siguientes:

Tabla 2. 2 Grupo de servicios a dar de alta

GRUPOS DE SERVICIOS		
Admon.IPCop	IPCop HTTPS	Habitual
	IPCop SSH	Habitual
	Ping	Habitual
Pto.Priv	Correo FAME	Habitual
	WebMail FAME	Habitual
	WebServices MP	Habitual
	Ping	Habitual
	Amigo Nuevo	Habitual
	pop3	Defecto
	pop3s	Defecto
	smtp	Defecto
	smtps	Defecto
	https	Defecto
Serv.IPCop	IPCop Proxy	Habitual
	Ping	Habitual
	domain	Defecto

Agrupamiento de direcciones: Esta opción permite realizar configuraciones por equipo, lo que representa mayor seguridad.

Fig. 2. 66 Agrupamiento de direcciones

Para este caso, se darán de alta el o los equipos que van a tener acceso al servicio de messenger, es posible añadir por dirección IP o por MAC.

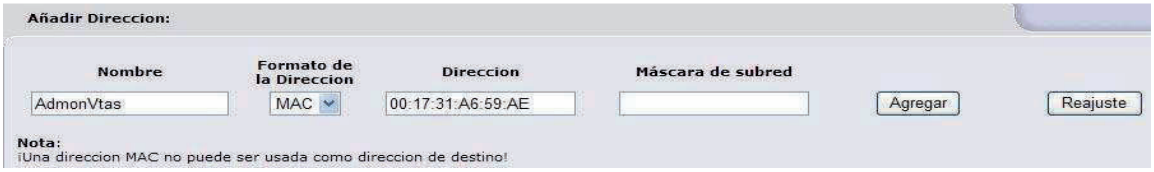


Fig. 2. 67 Añadir dirección para desbloqueo de messenger

2.4.5.1 Reglas

Las reglas deben ser creadas para permitir el tráfico y serán configuradas desde *Firewall/Bloquear tráfico de salida*, en la página se da clic sobre el botón Nueva Regla y en el formulario se introducen los datos correspondientes.

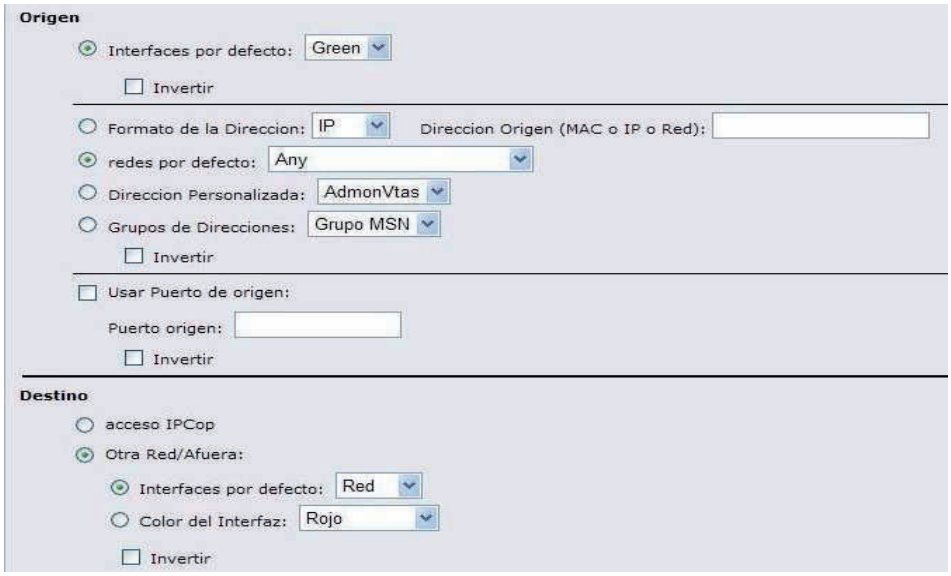


Fig. 2. 68 Configuración de reglas

Los datos solicitados se dividen en 4 secciones: Origen | Destino | Adicional | Añadir margen de tiempo. Las reglas principales para que IPCop no sea bloqueado en su totalidad son:

Tabla 2. 3 Reglas a dar la alta

ORIGEN	DESTINO	ADICIONAL	OBS
Interfaces por defecto: Green. Formato de la Dirección: IP. Dirección Origen: 192.168.0.0/16	Acceso IPCop. Interfaces por defecto: Red. Redes por defecto: Any. Usar servicio: Grupos de Servicios: *Admon.IPCop*	Regla habilitada. Regla de log.	Administración de IPCop
Interfaces por defecto: Green. Formato de la Dirección: IP. Dirección Origen: 192.168.37.0/24	Otra Red/Afuera. Interfaces por defecto: Red. Redes por defecto: Any Usar Servicio: Grupos de Servicios: *Pto.Priv*	Regla habilitada. Regla de log.	Puertos con Privilegios de Salida
Interfaces por defecto: Green. Redes por defecto: Green Network.	Acceso IPCop. Interfaces por defecto: Red. Redes por defecto: Any. Usar servicio: Grupos de Servicios: *Serv.IPCop*	Regla habilitada. Regla de log.	Servicios para salida a Internet

La primera regla permite que más de una máquina pueda entrar a la administración de IPCop. Abarca IPCop SSH que es necesario para administrar IPCop a través de SSH, IPCop https para el uso de WebGUI y el servicio de ping.

La segunda, incluye los servicios que permiten el envío y recepción de mensajes de correo, así como las páginas de navegación más usadas.

Y la tercera, permite la navegación por Internet a través del WebProxy de IPCop.

Las opciones adicionales se usan en caso de que se quiera que se registren los logs y la acción a realizar (aceptar o denegar) la regla, así como si sólo debe ser actividad en un momento determinado.

Finalmente, solo se activa el BlockOutTraffic.

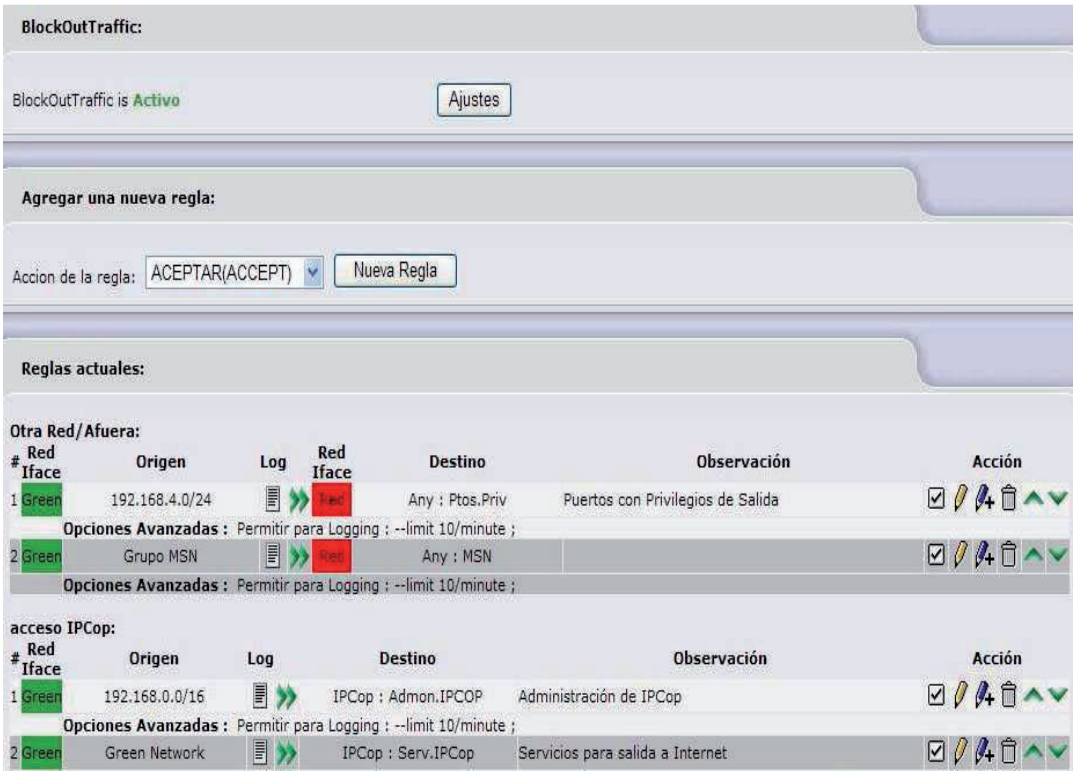


Fig. 2. 69 Activar BOT

Ahora IPCop está configurado para permitir BOT (BlockOutTraffic). Todo el tráfico que no esté permitido por las normativas vigentes estará bloqueado.

2.4.6 Logs

La página de Logs genera informes a partir de listas personalizadas y detalladas. En configuración de registro es posible dar las opciones para la visualización de los registros. En cada página existe la opción de habilitar Logs, lo que permitirá rastrear los accesos.

Los logs disponibles son:

- Configuración de registro. Configurar como se mostrarán los logs.
- Sumario de registro. Eventos de Kernel y estado de discos.
- Registro del proxy. Desde esta página se pueden ver las páginas que se han visitado.
- Registro de firewall. Registra eventos del firewall con dirección de origen, destino, MAC y puerto.
- Logs del filtro de URL. Páginas que han sido bloqueadas por el filtro de URL, indica el equipo y el motivo del bloqueo.
- Registros del sistema. Permite seleccionar sobre el servicio que sea necesario para mostrar los logs de suceso.

2.5 ACCESO REMOTO

Para el acceso remoto desde otra red del mismo dominio, es necesario dar a IPCop el comando necesario a través de la consola:

route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.X.X

Sin embargo, la siguiente vez que el equipo se reinicie se perderá la ruta. Para ello se edita el archivo rc.network, mediante el siguiente comando:

vi /etc/rc.d/rc.network

Este archivo muestra la configuración con la que arranca IPCop, así que en la última línea se agrega el comando, así el acceso remoto estará disponible aunque se reinicie IPCop.

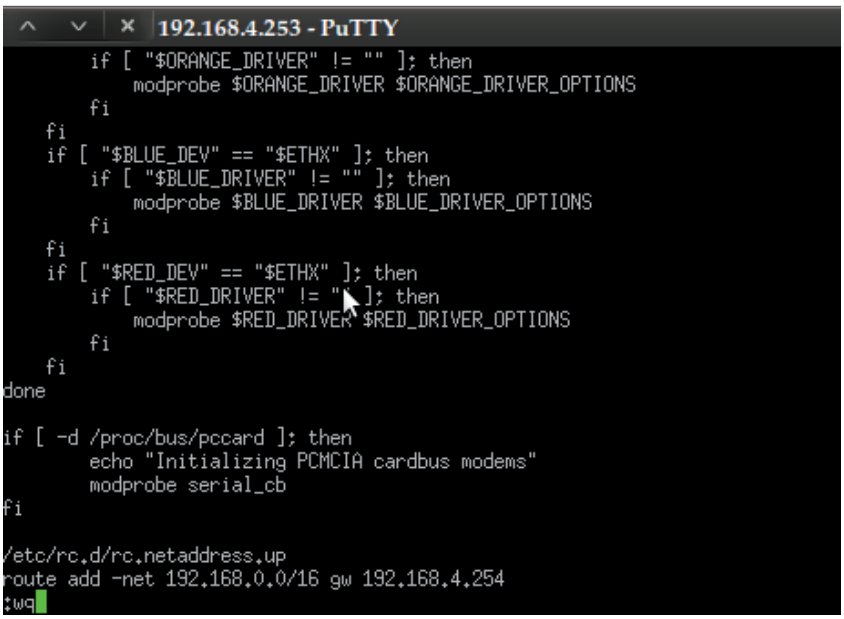


Fig. 2. 70 Acceso remoto en consola

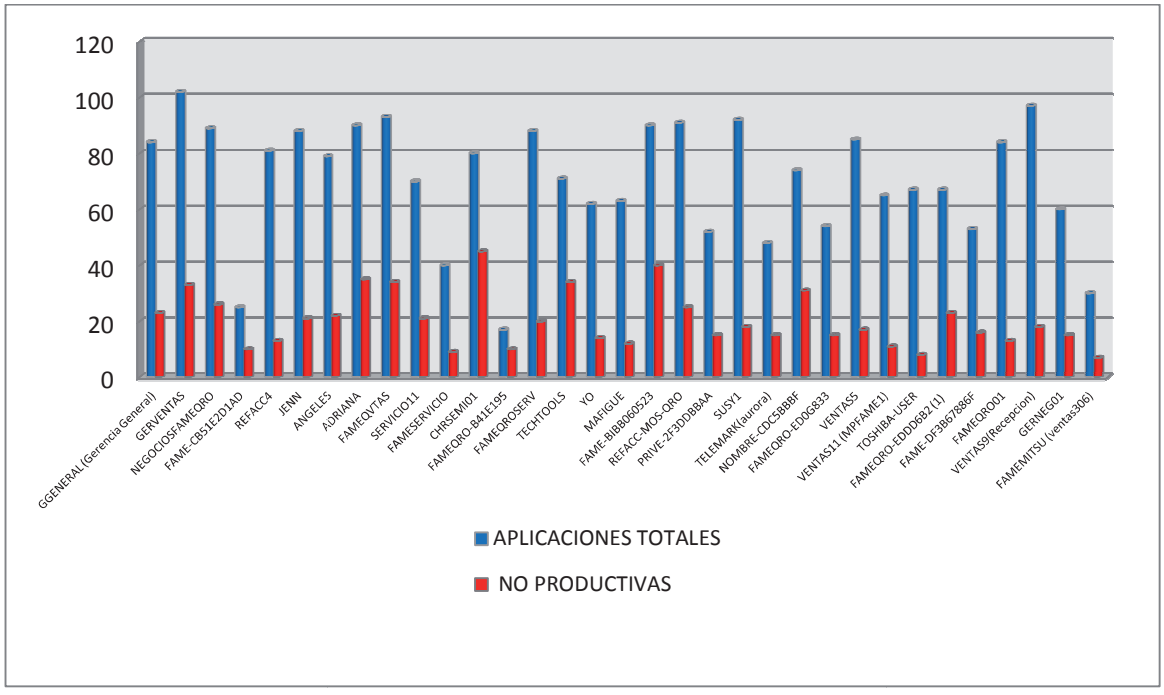
Con esta quedará abierta la conexión de otro equipo que se encuentre dentro de la misma red.

Capítulo 3 ANÁLISIS DE LOS RESULTADOS

Los resultados se comprobaron con estudios realizados antes y después de la implementación de IPCop. El análisis se realizó en todas las agencias de Grupo Fame, en este caso, se tomó como muestra a Fame Querétaro S.A. de C.V. la más grande del Grupo en el Estado de Querétaro, en el momento en el que se llevo a cabo (Enero 2010) contaban con un total de 33 equipos de cómputo.

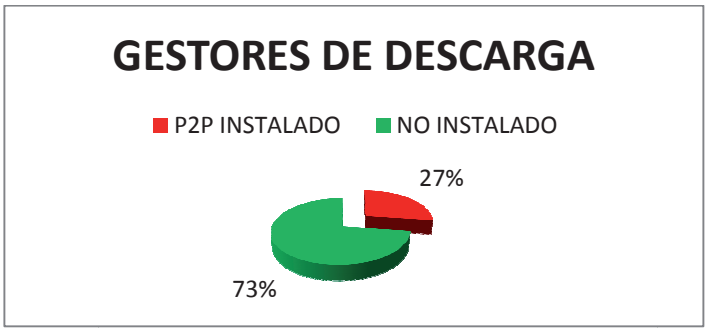
3.1 ANÁLISIS ANTES DE IPCOP

Para llevar a cabo el análisis, se realizaron auditorías para conocer a fondo la situación en que se encontraban los equipos. El primer reporte que se generó fue de la recopilación del total de aplicaciones que los usuarios tenían en los equipos, con enfoque a las aplicaciones que no debían estar instaladas por no ser parte de las funciones del trabajo.



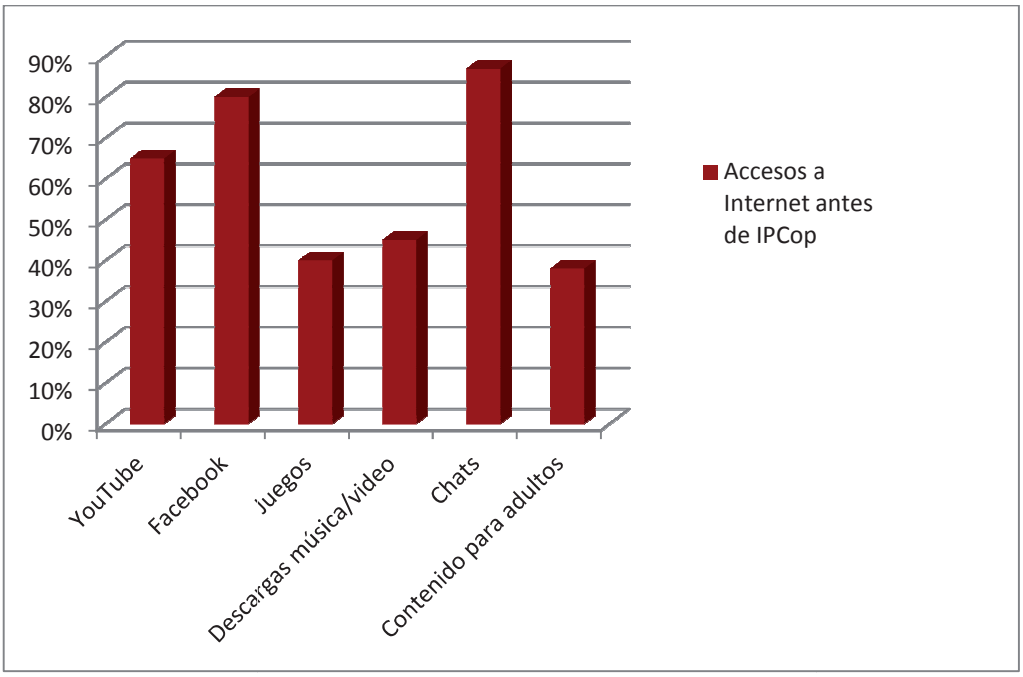
Gráfica 3. 1 Aplicaciones instaladas en PC´s

Posteriormente, se tomaron las aplicaciones no productivas para ver cuales afectaban más el rendimiento del equipo, encontrando que varios tenían programas P2P, que en gran medida son responsables del consumo de ancho de banda, siendo estos los resultados:



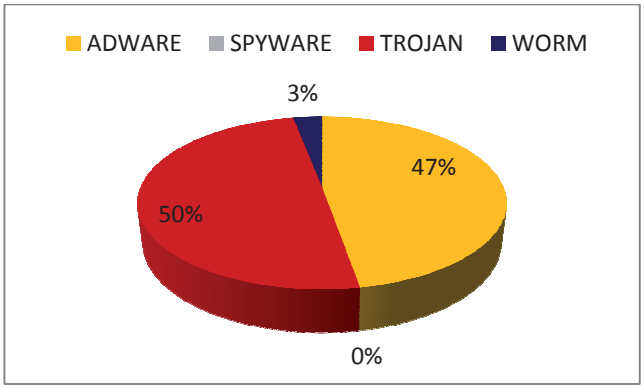
Gráfica 3. 2 Gestores de descarga instalados

Aparte de los programas instalados y como ya se ha mencionado, antes de la instalación del Firewall, cada estación de trabajo tenía acceso total a sitios de Internet, la mayoría de los usuarios aprovechaban para visitar cualquier cantidad de páginas durante el día. La siguiente gráfica muestra los accesos a sitios web antes de IPCop.



Gráfica 3. 3 Acceso a sitios

El acceso sin límite y las descargas de archivos provenientes de Internet, reflejaron los siguientes resultados de programas maliciosos en los equipos:



Gráfica 3. 4 Programas maliciosos detectados

Como resultado de lo anterior, nos encontramos con:

- Equipos lentos.
- Conexiones a Internet lentas e inseguras.
- Caídas del acceso a Internet.

Se consideraba la implementación de equipos Fortinet; aunque, en la Tabla 3.1 se muestra el costo que implicaría adquirir cada equipo.

Tabla 3. 1 Costo de implementar equipos Fortinet

TEQUIPO	LICENCIA	COSTO SIN IVA	INCLUIDO
Fortinet 	1 año	992 dólares	Equipo e instalación[4]

Una vez hecho este análisis, se procedió a hacer una depuración de programas y eliminación de virus en cada uno de los equipos, y se inicio la configuración de los Firewall con IPCop.

[4]Cotización 2012

3.2 ANÁLISIS DESPUÉS DE IPCOP

Actualmente Fame Querétaro cuenta con 47 equipos conectados a la red LAN. Se estandarizaron nombres de host, programas instalados y el inicio de sesión en los equipos.

Con IPCop podemos observar mediante las gráficas los horarios en los que el tráfico es mayor.

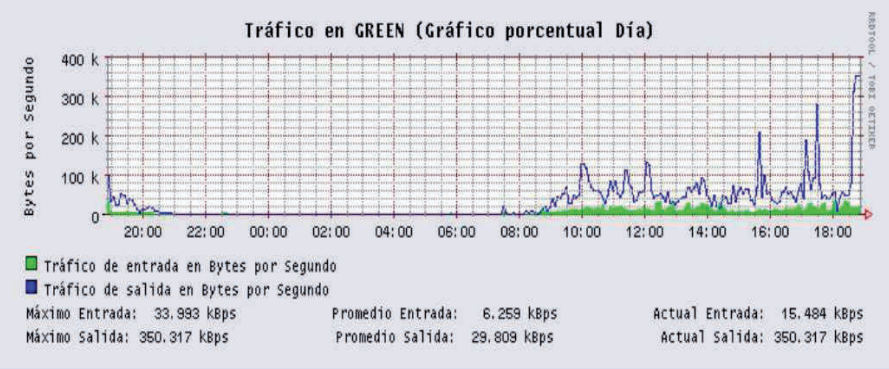


Fig. 3. 1 Tráfico en interfaz Verde

El servicio de DHCP permite identificar el nombre de los equipos, la IP y su MAC y con esto monitorear los accesos de los usuarios a Internet.

	00:02:e3:30:66:1e	192.168.4.51	D1QROFQRPC1106	12/10/2012 18:41:14
	c8:0a:a9:9a:51:65	192.168.4.52	D1QROFQRLT1118	12/10/2012 18:43:45
	00:08:74:f4:9f:e0	192.168.4.53	D1QROFQRPC1138	12/10/2012 18:57:21
	00:0d:56:04:0c:91	192.168.4.54	D1QROFQRPC1137	12/10/2012 18:32:58
	44:37:e6:9b:e2:96	192.168.4.55	D1QROFQRPC1115	12/10/2012 18:50:44
	00:17:31:a6:59:ae	192.168.4.56	D1QROFQRPC1111	12/10/2012 18:53:48
	44:37:e6:9b:a9:1a	192.168.4.57	D1QROFQRPC1121	12/10/2012 18:34:55
	00:17:31:a6:45:86	192.168.4.58	D1QROFQRPC1108	12/10/2012 18:37:55
	00:08:74:f7:7b:80	192.168.4.59	D1QROFQRPC1112	12/10/2012 18:44:50
	00:08:74:f4:a0:60	192.168.4.60	D1QROFQRPC1113	12/10/2012 18:45:32
	00:0f:fe:a4:fc:09	192.168.4.61	D1QROFQRPC1136	12/10/2012 18:28:49
	cc:52:af:44:1b:ac	192.168.4.62	D1QROFQRPC1122	12/10/2012 18:38:42
	00:08:74:f7:7c:68	192.168.4.63		~~11/10/2012 21:46:54~~
	00:08:74:f7:7b:2c	192.168.4.64	D1QROFQRPC1128	12/10/2012 18:28:37

Fig. 3. 2 Servidor DHCP

El Firewall permite la organización de páginas web sospechosas y maliciosas de tal forma que bloquea el acceso a este tipo de páginas y genera un reporte del número de eventos que han sido bloqueados como se muestra en la figura 3.3, por tiempo, categoría, cliente y destino.

16:46:02	downloads	192.168.4.70	client74.dropbox.com:443
16:46:03	chat	192.168.4.19	http://sn1msg3020330.gateway.messenger.live.com/gateway/gateway.dll?A...
16:46:03	chat	192.168.4.19	http://sn1msg3020330.gateway.messenger.live.com/gateway/gateway.dll?A...
16:46:03	chat	192.168.4.19	http://sn1msg3020330.gateway.messenger.live.com/gateway/gateway.dll?A...
16:46:04	chat	192.168.4.19	http://sn1msg3020330.gateway.messenger.live.com/gateway/gateway.dll?A...
16:46:17	tracker	192.168.4.6	sb.scorecardresearch.com:443
16:46:19	adv	192.168.4.6	view.atdmt.com:443
16:46:20	downloads	192.168.4.70	client41.dropbox.com:443
16:46:20	downloads	192.168.4.70	client82.dropbox.com:443
16:46:31	chat	192.168.4.70	geo.messenger.services.live.com:443
16:46:32	adv	192.168.4.70	ads1.msads.net:443
16:46:32	adv	192.168.4.70	ads1.msads.net:443
16:46:35	downloads	192.168.4.70	client37.dropbox.com:443
16:46:36	adv	192.168.4.70	h.atdmt.com:443
16:46:36	downloads	192.168.4.70	client8.dropbox.com:443
16:46:37	adv	192.168.4.70	h.atdmt.com:443
16:46:37	adv	192.168.4.70	h.atdmt.com:443
16:46:37	adv	192.168.4.70	h.atdmt.com:443
16:46:37	adv	192.168.4.70	flex.atdmt.com:443
16:46:44	chat	192.168.4.6	http://dps.msg.yahoo.com/ph/minty/?cb=phoneHomeCallback&intl=es&lang=...
16:46:50	tracker	192.168.4.6	http://b.scorecardresearch.com/p?c1=2&c2=7241469&c5=978520093&c7=http...
16:46:50	tracker	192.168.4.6	http://b.scorecardresearch.com/p?c1=2&c2=7241469&c5=978520273&c7=http...
16:46:53	chat	192.168.4.70	geo.messenger.services.live.com:443
16:46:54	chat	192.168.4.19	http://sn1msg3020330.gateway.messenger.live.com/gateway/gateway.dll?A...
16:46:54	downloads	192.168.4.70	client76.dropbox.com:443
16:46:54	downloads	192.168.4.70	client23.dropbox.com:443
16:46:55	adv	192.168.4.6	http://ad.yieldmanager.com/st?ad_type=iframe&ad_size=120x600,160x600&...
16:46:55	adv	192.168.4.6	http://ad.yieldmanager.com/st?ad_type=iframe&ad_size=180x150&site=154...
16:47:02	adv	192.168.4.19	http://bs.serving-sys.com/BurstingPipe/adServer.bs?cn=int&iv=2&int=11...
16:47:09	downloads	192.168.4.70	client18.dropbox.com:443
16:47:10	downloads	192.168.4.70	client69.dropbox.com:443
16:47:16	tracker	192.168.4.42	http://b.scorecardresearch.com/c2/9613729/cs.js
16:47:16	tracker	192.168.4.42	http://include.reinvigorate.net/re_.js
16:47:18	socialnet	192.168.4.42	http://platform.linkedin.com/in.js
16:47:26	custom-expressions	192.168.4.42	http://assets.animalpolitico.com/wp-content/plugins/facebook-comments...
16:47:26	custom-expressions	192.168.4.42	http://assets.animalpolitico.com/wp-content/plugins/facebook-comments...
16:47:27	downloads	192.168.4.70	client59.dropbox.com:443
16:47:53	socialnet	192.168.4.42	http://widgets.twimg.com/j/2/widget.js
16:47:54	tracker	192.168.4.42	http://edge.quantserve.com/quant.js
16:47:55	forum	192.168.4.42	http://static.typepad.com/.shared/v20121012.02-0-gef3def4/typepad/es ...
16:47:56	forum	192.168.4.42	http://www.typepad.com/t/comments?__mode=check_login
16:47:58	downloads	192.168.4.70	client39.dropbox.com:443
16:48:00	forum	192.168.4.42	http://platform.twitter.com/widgets.js
16:48:01	adv	192.168.4.42	http://ads.prisacom.com/RealMedia/ads/adstream_mix.ads/www.elpais.es/...
16:48:01	tracker	192.168.4.42	http://prisacom.112.2o7.net/b/ss/prisacomelpaiscom,prisacomglobal/1/H...
16:48:02	downloads	192.168.4.70	client36.dropbox.com:443
16:48:03	adv	192.168.4.42	http://ads.prisacom.com/RealMedia/ads/adstream_nx.ads/www.elpais.es/b...
16:48:03	adv	192.168.4.42	http://ads.prisacom.com/RealMedia/ads/adstream_nx.ads/www.elpais.es/b...

Fig. 3. 3 Log del filtro de URL

En el sumario de registro, vemos la cantidad de paquetes TCP que son registrados de cada uno los equipos en la LAN.

```
Logged 4154 packets on interface eth0
  From 192.168.4.1 - 9 packets to tcp(8889)
  From 192.168.4.3 - 1 packet to tcp(8889)
  From 192.168.4.4 - 68 packets to tcp(8889)
  From 192.168.4.5 - 3 packets to tcp(8889)
  From 192.168.4.6 - 18 packets to tcp(8889)
  From 192.168.4.10 - 75 packets to tcp(8889)
  From 192.168.4.11 - 19 packets to tcp(8889)
  From 192.168.4.14 - 11 packets to tcp(8889)
  From 192.168.4.16 - 9 packets to tcp(443,8889)
  From 192.168.4.18 - 183 packets to tcp(8889)
  From 192.168.4.19 - 135 packets to tcp(443,8889)
  From 192.168.4.20 - 369 packets to tcp(8889)
  From 192.168.4.21 - 112 packets to tcp(8889)
  From 192.168.4.23 - 77 packets to tcp(8889)
  From 192.168.4.24 - 1 packet to tcp(8889)
  From 192.168.4.25 - 15 packets to tcp(443,8889)
  From 192.168.4.26 - 24 packets to tcp(8889)
  From 192.168.4.27 - 108 packets to tcp(443,8889)
  From 192.168.4.29 - 29 packets to tcp(8889)
  From 192.168.4.30 - 1 packet to tcp(443)
  From 192.168.4.32 - 178 packets to tcp(443,8889)
  From 192.168.4.33 - 87 packets to tcp(8889)
  From 192.168.4.34 - 32 packets to tcp(8889)
  From 192.168.4.35 - 25 packets to tcp(443)
```

Fig. 3. 4 Paquetes TCP

IPCop nos permite identificar los sitios con mayor número de accesos, como se muestra en la figura 3.5, y de esa forma bloquear los que no se permitan.

```
# Request-destinations by 2nd-level-domain
destination                              request     %    Byte      %   hit-%
---------------------------------------- --------- ------ -------- ------ ------
<error>                                     1996  17.60      3M   2.70  15.53
*.consulta-its.com                          1980  17.46      1M   0.53   0.00
*.anunciosred.com.mx                         748   6.60     22M  17.60   0.00
*.clasificadoscontacto.com                   566   4.99     16M  12.53   6.71
*.yimg.com                                   454   4.00      6M   4.82  21.81
*.google.com.mx                              422   3.72      7M   5.55  14.93
*.live.com                                   399   3.52      5M   4.16   4.01
*.gstatic.com                                332   2.93      2M   1.57   4.82
*.yahoo.com                                  297   2.62      1M   0.81   1.35
*.microsoft.com                              269   2.37      1M   0.79  13.38
*.chrysler.com                               219   1.93      4M   3.56   4.11
*.wlxrs.com                                  203   1.79      2M   1.35  71.92
*.msn.com                                    202   1.78      3M   2.32   0.00
*.s-msn.com                                  196   1.73      2M   2.01  64.29
*.msecnd.net                                 169   1.49      7M   5.43  18.34
*.inter-chat.com                             168   1.48      0M   0.15   0.00
trabajoypersonal.com                         167   1.47      1M   0.54  65.27
*.jornada.unam.mx                            161   1.42      2M   1.59   0.00
*.hotmail.com                                124   1.09      1M   0.88  61.29
*.windowsupdate.com                          119   1.05      0M   0.18  26.89
*.avg.com                                    118   1.04      1M   0.58   0.00
*.atdmt.com                                  103   0.91      0M   0.13   0.00
*.google.com                                 101   0.89      3M   2.21   4.95
*.intel.com                                  100   0.88      1M   0.80   0.00
*.google-analytics.com                        90   0.79      0M   0.11   0.00
other: 155 2nd-level-domains                1636  14.43     34M  27.11   5.68
---------------------------------------- --------- ------ -------- ------ ------
Sum                                        11339 100.00    124M 100.00  10.66
```

Fig. 3. 5 Calamaris, reporte de proxy

Como las páginas de chat no están permitidas, bloqueamos el acceso en el filtro de URL como se muestra en la figura 3.6.

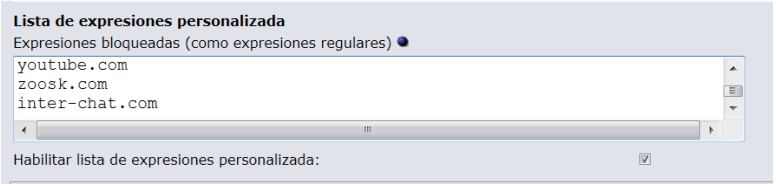


Fig. 3. 6 Bloqueo de expresiones

Sitios como youtube, facebook, páginas de juegos, descargas, chat, sitios con contenido para adultos quedaron bloqueados. Con lo que conseguimos tener una red estable, las caídas de Internet que se han presentando se han debido a problemas técnicos con el proveedor de servicios.

CONCLUSIÓN

La implementación del Firewall se concluye de manera satisfactoria, ha funcionado 3 años sin interrupción y sin complicaciones, porque lo que se confirma que es un sistema bastante estable y confiable.

Con IPCop se consiguió tener un servicio de red que brindara seguridad en la comunicación a través de Internet. Además de no requerir de un gran presupuesto por ser Software Libre y con la posibilidad de aprovechar equipo obsoleto.

BIBLIOGRAFÍA

Básicamente se ha utilizado internet como fuente de información a continuación se enumeran los enlaces:

[1] http://www.ipcop.org visitado de noviembre de 2009 a febrero de 2010

[2] http://dns.bdat.net/documentos/squid/x243.html visitado en enero de 2010

[3] http://winscp.net/eng/download.php visitado en noviembre de 2009

[4] Fuente: TUX Info nro 7 visitado en marzo de 2011

[5] http://es.wikipedia.org/wiki/IPCop visitado en abril de 2011

[6] http://www.sudano.net/configuracion-y-administracion-basica-de-ipcop/ visitado en abril de 2011

[7] http://www.snort.org/ visitado en abril de 2011

[8] http://www.netfilter.org/ visitado en abril de 2011

[9] http://www.linux.org.es visitado en mayo de 2011

[10] http://www.monografias.com/trabajos15/firewall-linux/firewall-linux.shtml visitado en mayo de 2011

[11] http://www.alegsa.com.ar/Notas/261.php visitado en mayo de 2011

[12] http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29 visitado en mayo de 2011

[13] http://dns.bdat.net/documentos/squid/x243.html visitado en mayo de 2011

[14] http://ArkandaSOS.com visitado en enero de 2012

[15] http://www.drea.co.cr/innovaciones_educativas/Compartiendo/Firewall%20IP%20COP%20Linux.pdf visitado en enero de 2012

[16] http://www.monografias.com/trabajos/solinux/solinux.shtml visitado en enero de 2012

[17] http://www.bilib.es/recursos/analisis-de-aplicaciones/analisis/doc/analisis-de-aplicacion-cortafuegos-de-ipcop/ visitado en enero de 2012

[18] http://www.wadalbertia.org/foro/viewtopic.php?f=4&t=92&start=0 visitado en enero de 2012

[19] http://www.maginvent.org/articles/linuxmm/Ventajas_Linux.html visitado en enero de 2012

[20] http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29 visitado en marzo de 2012

[21] http://windows.microsoft.com/es-XL/windows-vista/Exploring-the-Internet visitado en marzo de 2012

[22] http://es.wikipedia.org/wiki/Proxy visitado en marzo de 2012

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICAS

GLOSARIO DE TÉRMINOS

ANCHO DE BANDA: Cantidad de datos que pueden ser transportados por algún medio en un determinado período de tiempo (generalmente segundos).

DHCP: (Siglas en inglés de *Dynamic Host Configuration Protocol*, en español "protocolo de configuración dinámina de host") es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

DMZ: Zona desmilitarizada. Se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.

FTP: Siglas en inglés de *File Transfer Protocol*, en español "protocolo de transferencia de

GUI: Siglas en inglés de *Graphical User Interface*, es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.

HOST: Se refiere a las computadoras conectadas a una red, que proveen y utilizan servicios en ella.

HTTP: (Siglas en inglés de *Hyper Text Transfer Protocol*, en español "protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la WWW.

ICMP: Siglas en inglés de *Internet Control Message Protocol*, es el protocolo de mensajes de Internet.

IMAP: Siglas en inglés de *Internet Massage Access Protocol*, es un protocolo de aplicación de acceso a mensajes electrónicos almacenados en un servidor.

INTERFAZ: Elemento de comunicación/conexión, entre dos sistemas o dispositivos.

IP: Protocolo de Internet. Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz de un dispositivo.

ISO: Es un archivo donde se almacena una copia o imagen exacta de un sistema de ficheros.

ISP: Siglas en inglés de *Internet Service Provider,* en español proveedor de servicios de Internet.

MIME: Siglas en inglés de *Multipurpose Internet Mail Extensions,* en español extensiones multipropósito de correo de Internet.

POP3: (Siglas en inglés de *Post Office Protocol*, en español "protocolo de oficina postal"), se utiliza en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto.

PPPOE: (Siglas en inglés de *Point-to-Point Protocol Over Ethernet*, en español "protocolo punto a punto sobre Ethernet), es un protocolo de red para la encapsulación PPP sobre una capa de ethernet.

PROXY: Es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina **A** solicita un recurso de una **C**, lo hará mediante una petición a **B**; **C** entonces no sabrá que la petición procedió originalmente de **A**.

RDSI: Red Digital de Servicios Integrados.

RED: Es cualquier sistema de computación que enlaza dos o más equipos.

SMTP: Siglas en inglés de *Simple Mail Transfer Protocol,* en español protocolo para la transferencia simple de correo electrónico.

SSH: Siglas en inglés de *Secure SHell,* en español intérprete de órdenes segura.

TCP: Siglas en inglés de *Transmission Control Protocol*, en español Protocolo de Control de Transmisión.

VPN: Siglas en inglés de *Virtual Private Network*, en español red privada virtual.

WWW: Siglas en inglés de World Wide Web, es español red informática mundial.