Manual del Administrador de IPCop v2.0.0

Jesús Ezquieta

16 de Junio de 2013

Historial de revisiones		
Revisión 2.x	2009-2013	JE
Añadidos y modificaciones de IPCop v2		

Tabla de contenidos

Lista de figuras

Lista de tablas

1. Derechos y Renuncias

1ª Edición - 29 de Diciembre de 2001

Editor Charles Williams

Me gustaría agradecer a la gente que ha revisado y corregido el documento: Harry Goldschmitt, Mark Wormgoor, Eric S. Johansson y el resto del IPCop Linux Group.

2ª Edición - 10 de Enero de 2003

Editores - Chris Clancey, James Brice, Harry Goldschmitt, and Rebecca Ward

3ª Edición - 25 de Abril de 2003

Editores - Chris Clancey, Harry Goldschmitt, and Rebecca Ward

4ª Edición - 25 de Septiembre de 2004

Editores - Chris Clancey, Harry Goldschmitt, John Kastner, Eric Oberlander and Peter Walker

Traducción al Español - Junio 2013

Traductor - Jesús Ezquieta

2. Presentación

Hola. En nombre de nuestro Líder de Proyecto, Jack Beglinger, el personal de Documentación quiere darte la bienvenida al Manual del Administrador de IPCop. Nos gustaría aprovechar esta oportunidad para agradecerte que pruebes nuestro cortafuegos y esperamos que cubra tus necesidades. El equipo agradece también a la Comunidad de IPCop Linux por su presencia continuada y el magnífico trabajo que hace ayudando tanto a los nuevos usuarios como a los ya experimentados. También nos gustaría dar las gracias al equipo de SmoothWall por unirse a la Comunidad de IPCop Linux.

Tanto si eres un usuario existente actualizando la versión o un nuevo usuario listo para tu primera instalación, esperamos que encuentres todo lo que necesitas para ponerte en marcha en este manual. Si por alguna razón, algo no está cubierto aquí y crees que debería estarlo, no dudes en contactarnos

y hacérnoslo saber. Siempre nos gusta escuchar a nuestra base de usuarios (de hecho, algunos de nosotros estamos bastante solos, sentados delante del ordenador todo el día y una pequeña nota es agradable de vez en cuando) y esperamos poder acomodarnos a sus necesidades tanto como nos sea posible. Ahora puedes relajarte y disfrutar de Internet sin tener que preocuparte.

Así que aquí presentamos algo de información para aquellos de vosotros que tengan tiempo para leer esto y deseamos que instaleis vuestra máquina IPCop. El lanzamiento inicial de IPCop fue un lanzamiento provisional para ayudarnos a encontrar problemas en la Distribución IPCop Linux. Ahora estamos en nuestro cuarto lanzamiento completo. Si tuvieras problemas, por favor, echa un vistazo a las FAQ lo primero, ya que tratamos de mantener las FAQ actualizadas tan pronto como encontramos un problema y podemos aportar información sólida bien para una solución temporal o para una corrección directamente.

Si tu problema no aparece en las FAQ puedes unirte a nosotros en IRC (servidor: irc.freenode.net channel: #ipcop), contactarnos mediante la lista de correo IPCop-User o utilizar uno de los foros de la Comunidad.

Puede que encuentres más información y las FAQ más actuales, información sobre listas de correo e información de contacto del IPCop Linux Group en nuestra web: IPCop Web Site

1.1. ¿Qué es IPCop?

Ahora, ¿qué es IPCOp?

1. IPCop es un cortafuegos; de principio, de final y siempre.
2. IPCop es una Distribución Linux especializada; completa, configurada y lista para proteger su red. Además, está distribuida bajo licencia GNU General Public License, con todo el código fuente disponible para descargarlo, revisarlo o incluso ser modificado y/o recompilado por usted mismo para sus necesidades personales o por razones de seguridad.
3. IPCop es una comunidad; donde los miembros se ayudan entre sí, compartiendo para mejorar el proyecto y entre ellos. Esta ayuda va desde simples instrucciones y consejos del “Networking básico”, hasta ayudar a los miembros a personalizar su IPCop para cubrir una necesidad especial como los teléfonos IP (VoIP) o la integración de múltiples oficinas.

Esta era una pregunta compleja. La respuesta es: todo lo anterior.

Trasfondo:

IPCop creció por múltiples necesidades. La primera de esas necesidades era la protección segura de nuestras redes personales y comerciales. Cuando IPCop empezó, en Octubre de 2001, había otros cortafuegos disponibles. De todas formas, el equipo que empezó IPCop sentía que las otras dos necesidades que IPCop cubre no estaban conseguidas; GPL y un sentido de comunidad.

El grupo fundador de IPCop decidió hacer las cosas de forma diferente y ramificó el código GPL de un cortafuegos existente para empezar uno nuevo, cuidando de mantener las necesidades de la comunidad de usuarios en primer término. Entre estas necesidades está la capacidad del usuario para hacer su propio IPCop, para instalar mejoras, para simplemente aprender viendo lo que otros han hecho. A través de estas necesidades es donde el desarrollo aporta mejoras a IPCop, escuchando directamente y viendo lo que se ha hecho y el porqué. Esta comunidad hace que IPCop crezca y IPCop la hace crecer.

Avanzamos hasta 2011. Unos 10 años después, millones de descargas y un número incontable de instalaciones por todo el mundo, se ha liberado una nueva versión de IPCop. Con IPCop v2.0.0, se han añadido algunas cosas estupendas, una interfaz rediseñada y un cortafuegos de salida, por nombrar algunas.

Así que de nuevo, ¡bienvenido a IPCop!

1.2. Lista parcial de prestaciones

- Filtros de red IPTables
- Soprte para discos IDE, SATA, SCSI y CF (Disk on a Chip). Con RAID por software opcional.
- Soporte para cuatro redes:
  - VERDE — Red interna de confianza
  - AZUL — Red inalámbrica semi-confiable (puede usarse como una segunda VERDE)
  - NARANJA — DMZ para servidores accesibles desde Internet
  - ROJA — La red conectada a Intenet mediante:
    - Módem analógico
    - RDSI
    - Conectado a una tarjeta de red:
      - Módem DSL
      - Cable Módem
    - Conectado por USB (con el driver adecuado):
      - Módem DSL
      - Cable Módem
- Soporte para Múltiples IPs “Real” en ROJA cuando se usan IPs estáticas.
- Soporte de cliente DHCP en ROJA para recibir una IP del ISP, también soportando la actualización de un DNS dinámico cuando esta IP cambia.
- Servidor DHCP para VERDE y AZUL para simplificar la configuración y el mantenimiento de la red.
- Servidor y cliente NTP para ajustar el reloj de IPCop y proveer un reloj común para las redes VERDE y AZUL.
- Red Privada Virtual (VPN) para permitir a múltiples localizaciones actuar como una única gran red.
- Red Privada Virtual (VPN) para permitir a los usuarios remotos acceder a la sede principal (RoadWarrior).
- Un Proxy tanto para navegar la Web como DNS permite una respuesta de conexión “más rápida” y una configuración de red simplificada.
- La Administración tras la carga inicial es mediante una interfaz Web segura, que incluye:
  - Gráficos de rendimiento de CPU, memoria y disco, así como de tráfico de red
  - Vista de registros con autorotación.
  - Soporte multilenguaje.
- Uso de equipos antiguos. 486 o superior, tamaño de disco mínimo de 512 MB y al menos 64 MB de RAM.

1.3. ¿Qué hay nuevo en la v2.0?

IPCop v2.0 es un desarrollo de la v1.4, pero incorpora algunas mejoras significativas.

- Núcleo Linux 2.6.32
- Nuevo soporte de hardware, incluyendo plataformas Cobalt, sparc y PPC.
- Nuevo instalador, que le permite instalar sobre discos flash o discos duros y seleccionar las tarjetas de red y asignarlas a cada red en particular.
- El acceso a **todas** las páginas web de la interfaz está ahora protegido con contraseña.
- El puerto para conexiones seguras https se ha cambiado al **8443**.

  La redirección de los puertos 81 y 445 no funcionará.
- Una nueva apariencia de la interfaz de usuario, que incluye:
  - Una nueva página Programador en el menú Sistema, donde puede programar varios eventos.
  - Más páginas en el menú Estado incluyendo nuevas páginas para Información del Sistema, Recuento de Tráfico, y IPTables, así como una página para Conexiones revisada.
  - Una página de Proxy actualizada, ahora con prestaciones de control avanzadas.
  - Hay una página de Servidor DHCP simplificada. Y por debajo, **dnsmasq** ha sido sustituido por **dhcpd** como servidor DHCP.
  - La página Servidor de Hora también ha sido simplificada, ya que IPCop usa ahora **ntpd** para todo.
  - Todo el Menú de Cortafuegos se ha revisado, y los 'pinholes' y redirecciones de puertos ahora se controlan mediante Reglas de Cortafuegos.
  - OpenVPN se ha añadido a IPCop como alternativa a IPsec.
- Por otro lado, el Sistema de Detección de Intrusiones **snort** se ha eliminado desde IPCop v2.0, para pasar a ser un añadido.

IPCop v2.1 incorpora correción de errores y algunas mejoras más:

- Núcleo Linux 3.0.41
- Servicio URL filter.

1.4. Agradecimientos

El software IPCop es tanto un proyecto colaborativo como un desarrollo a partir de un gran trabajo anterior. Estos agradecimientos abarcarán a muchos de los que ayudan, directa o indirectamente, pero no obstante faltarán algunos que trabajaron para ayudar a desarrollar este proyecto pero que no figuran aquí. Para ellos, muchas gracias y perdón por olvidar vuestro nombre.

Para el resto, gracias... Para un listado más actual, vea los Créditos en IPCop.

Equipo principal

- Olaf Westrik — Coordinador de liberaciones
- Achim Weber — Desarrollador
- Alan Hourihane — Desarrollador
- Eric Oberlander — Desarrollador

- Gilles Espinasse — Desarrollador
- Ivan Kabaivanov — Desarrollador
- Marco Sondermann — Desarrollador
- Mark Wormgoor — Desarrollador
- Robert Kerr — Desarrollador
- Ufuk Altinkaynak — Desarrollador
- Seth Bareiss — Gráficos
- Tom Eichstaedt — Gráficos

Documentación. Harry Goldschmitt, Chris Clancey, John Kastner, Eric Oberlander, Peter Walker

Traductores.

- **Coordinador de Traducciones:** Eric Oberlander
- **Desarrollador de la Base de Datos de la Web de Traducciones:** Marco van Beek
- **Africano:** Johann du Preez
- **Alemán:** Dirk Loss, Ludwig Steininger, Helmet, Markus, Michael Knappe, Michael Linke, Richard Hartmann, Ufuk Altinkaynak, Gerhard Abrahams, Benjamin Kohberg, Samuel Wiktor, Tom Eichstaedt
- **Árabe:** Ghalia Saleh Shariha, Salma Mahmod Ashour
- **Búlgaro:** Alexander Dimitrov
- **Catalán:** Albert Ferran Casas, Sergi Valls, Josep Sanchez, Toni
- **Checo:** Petr Dvoracek, Jakub Moc
- **Chino (Simplificado):** Vince Chu, Yuan-Chen Cheng, Sohoguard
- **Chino (Tradicional):** Ronald Ng
- **Danés:** Michael Rasmussen, Daniel Hammer, Morten Christensen
- **Eslovaco:** Miloš Mráz, Drlik Zbynek
- **Esloveno:** Miha Martinec, Grega Varl
- **Español** Curtis Anderson, Diego Lombardia, Mark Peter, Quique Soriano, David Cabrera Lozano, Jose Sanchez, Santiago Cassina, Marcelo Zunino, Alfredo Matignon, Juan Janczuk, Vicente Javier Garcia Mayen, Ricardo Lopez, Enrique Porta, Jesús Ezquieta
- **Español Latino:** Fernando Diaz
- **Finlandés:** Kai Käpölä
- **Francés:** Bertrand Sarthre, Michel Janssens, Erwann Simon, Patrick Bernaud, Marc Faid'herbe, Eric Legigan, Eric Berthomier, Stéphane Le Bourdon, Stéphane Thirion, Jan M. Dziewulski,spoutnik, Eric Darriak, Eric Boniface, Franck Bourdonnec, Jean Pierre Bargheon, Guy Godin
- **Griego:** Spyros Tsiolis, A. Papageorgiou, G. Xrysostomou
- **Gujarati:** Kartik Mistry
- **Holandés:** Gerard Zwart, Berdt van der Lingen, Tony Vroon, Mark Wormgoor, Maikel Punie and Bjorn Kaag
- **Húngaro:** Ádám Makovecz, Ferenc Mányi-Szabó

- **Italiano:** Fabio Gava, Antonio Stano, Marco Spreafico, Alessio Cecchi, Gabrielle Bellini, Massimiliano Neri
- **Japonés:** Adam Barbary Raina Otoni
- **Lituano:** Aurimas Fišeras, Rodion Kotelnikov
- **Noruego:** Morten Grendal, Alexander Dawson, Mounir S. Chermiti, Runar Skraastad, Alf-Ivar Holm
- **Persa (Farsi):** Ali Tajik, A T Khalilian
- **Polaco:** Jack Korzeniowski, Piotr, Andrzej Zolnierowicz, Remi Schleicher
- **Portugués:** Luis Santos, Renato Kenji Kano, Mark Peter, Wladimir Nunes, Daniela Cattarossi
- **Portugués de Brasil:** Edson-Empresa, Claudio Corrêa Porto, Adilson Oliveira, Mauricio Andrade, Wladimir Nunes
- **Rumano:** Viorel Melinte
- **Ruso/Ucraniano:** Vladimir Grichina, Vitaly Tarasov, Nikolay Parukhin
- **Somalí:** Mohamed Musa Ali
- **Sueco:** Anders Sahlman, Christer Jonson
- **Tailandés:** Touchie
- **Turco:** Ismail Murat Dilek, Emre Sumengen, Caglar Ulkuderner
- **Urdu:** Mudassar Iqbal
- **Vietnamita:** Le Dinh Long

Otros proyectos y Compañías. Traverse Technologies — soporte mejorado para doble RDSI y DOV, Linux from Scratch (LFS) — Código Base para 1.4, FreeSwan y OpenFreeSwan — software IPSec y VPN, Smoothwall — fundamentos e inspiración originarios, …y otros demasiado numerosos para mencionarlos.

2.1. Página de inicio de Administración

Acceder a la interfaz de IPCop es tan sencillo como abrir su navegador e introducir la dirección IP (de la interfaz VERDE) o el hostname de su IPCop, añadiendo el puerto https: https://ipcop.localdomain:8443 o https://192.168.1.1:8443.

Abandono de los puertos 81 y 445

Desde la versión 2.0.0, las conexiones http al puerto 81 **no** se redireccionan a un puerto seguro.

También, desde la versión 2.0.0, el puerto para las conexiones seguras https se ha cambiado al **8443**. Las conexiones al puerto 445 **no** serán redireccionadas.

Cambiando el puerto HTTPS

La utilidad de línea de comandos **setreservedports** para permitir a los Administradores cambiar el puerto seguro. Vea la sección setreservedports para más detalles.

Se le pedirá un nombre de usuario y una contraseña. Utilice `admin` como nombre de usuario, y la contraseña que eligió durante la instalación de IPCop.

Ahora debería estar viendo la pagina de inicio de la Administración de su IPCop. Puede empezar a explorar las diferentes opciones y la información disponible a través de esta interfaz.

Figura 2.1. Página de inicio

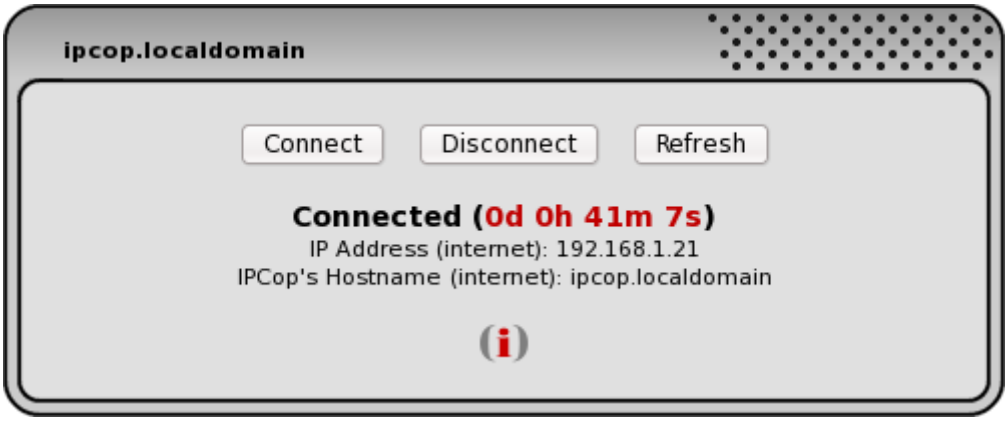
Al pie de cada página podrá ver un icono de Sourceforge que enlaza a los recursos del proyecto en Sourceforge. El pie de página también muestra el estado de conexión actual, sobre la fecha y hora, y el número de versión del sistema instalado, además de la nota de copyright. A mano derecha, el icono de Tux con escudo enlaza a la web de IPCop.

Las Páginas de Administración (PA) están disponibles a través de los menús en la parte alta de la pantalla.

- Sistema - Configuración del sistema y funciones de las utilidades asociadas al propio IPCop.
- Estado - Muestra información detallada del estado de varias secciones de su IPCop.
- Red - Se emplea para la configuración y administración de los ajustes de marcado y/o PPP.
- Servicios - Configuración y administración de muchas opciones de los servicios de su IP-Cop.
- Cortafuegos - Configuración y administración de las reglas del cortafuegos de IPCop.
- VPNs - Configuración y administración de los ajustes y opciones de las redes virtuales privadas (VPNs) de su IPCop.
- Registros - Vea todos los registros de su IPCop (cortafuegos, proxy, etc.)

La página de inicio de IPCop es una de las páginas que variarán en función de cómo esté configurado IPCop. Si su conexión a Internet es mediante una interfaz ROJA Ethernet, la página de inicio no mostrará un nombre de conexión (el 'Perfil Actual').

Figura 2.2. Página de inicio - Conexión Ethernet



Si todo fue bien durante la configuración de su conexión PPP, y el tipo de conexión empleado para conectarse a Internet es PPP, verá una caja similar a la siguiente.

Figura 2.3. Página de inicio - Conexión por módem

Nota

No verá ninguna conexión activa hasta que haya terminado de configurar su IPCop.

En la esquina superior izquierda de la caja verá el nombre de dominio de su IPCop.

Hay tres botones en la caja. Dos controlan la conexión a Internet:

- Conectar - Fuerza un intento de conexión a Internet.
- Desconectar - Desconecta la conexión a Internet.
- Actualizar - Fuerza una actualización de la página para actualizar los datos.

Además de los anteriores botones, verá el “Perfil Actual” que se está empleando para conectarse a Internet(definido en la página de Marcado). Bajo la línea “Perfil Actual” verá el estado actual de su conexión. Será uno de los siguientes:

- Desconectado - No hay conexión a Internet y no se está intentando conectar.
- Marcando - Intentando conectar a Internet.

- Conectado - Actualmente conectado a Internet.
- Marcado bajo demanda en espera - Actualmente no conectado a Internet. Esperando actividad de un cliente en la red para iniciar una conexión.

Si está actualmente conectado a Internet, verá una línea de Estado de conexión con el siguiente formato:

- Conectado (#d #h #m #s)
- d=Días conectado
- h=Horas conectado
- m=Minutos conectado
- s=Segundos conectado

IPCop tiene dos usuarios web. El primero se llama 'admin'. Autenticarse como este usuario otorga acceso a todas las Páginas de Administración. El otro usuario, llamado 'dial', sólo puede usar los botones Conectar o Desconectar. por defecto, el usuario 'dial' está deshabilitado. Para habilitarlo debe asignar una contraseña a ese usuario.

Abandono del acceso GUI sin autenticación

Desde la versión 2.0.0 de IPCop, **debe** estar autenticado para acceder a la GUI. Esto incluye las páginas de inicio y de créditos.

2.2. Páginas web de Sistema

Este grupo de páginas web está diseñado para ayudarle a administrar y controlar el propio IPCop. Para llegar a estas páginas, seleccione Sistema de la barra de pestañas en lo alto de la pantalla. Aparecerán las siguientes opciones en un desplegable:

- Inicio — Vuelve a la página de inicio.
- Programador — Le permite programar eventos de reinicio, apagado, conexión y desconexión en IPCop.
- Actualizaciones — Le permite buscar y aplicar correcciones a IPCop.
- Contraseñas — Le permite definir la contraseña de 'admin' y, opcionalmente, la de 'dial'.
- Acceso SSH — Le permite activar y configurar 'Secure Shell', acceso SSH a IPCop.
- Ajustes GUI — Activa o desactiva el uso de JavaScript y le permite definir el idioma en el que se muestra la interfaz web.
- Ajustes de correo — Ajustes globales para el envío de correos.
- Copia de seguridad — Haga una copia de seguridad de los ajustes de su IPCop, bien a un archivo o a un disquete. También puede restaurar sus ajustes desde esta página.
- Apagado — Apague o reinicie su IPCop desde esta página.

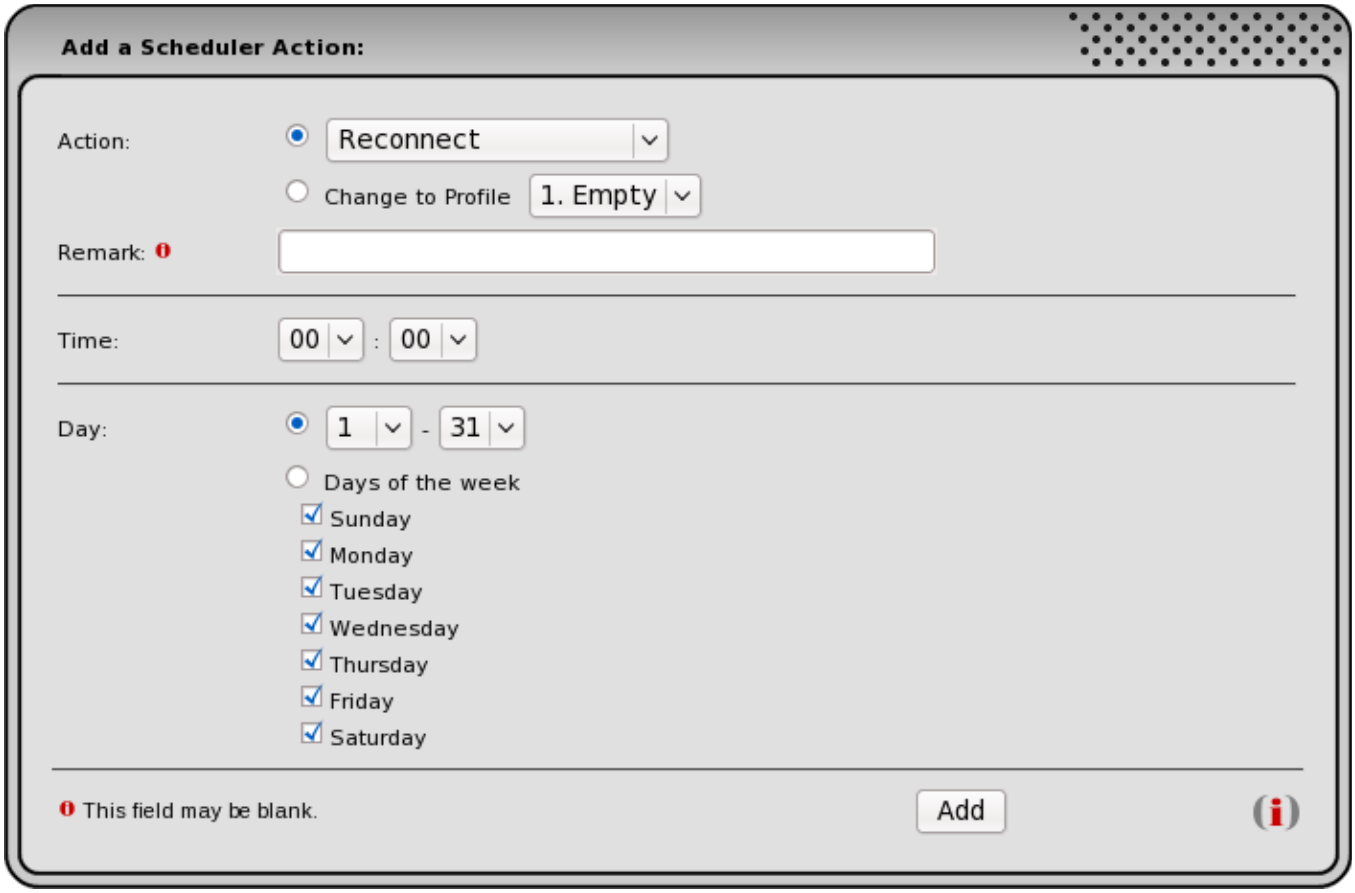
- Créditos — Esta página lista los muchos voluntarios y otros proyectos que hacen tan grande a IPCop.

2.2.1. Programador

Esta página tiene dos secciones:

1. La primera sección le permite Añadir o Editar un evento programado.
2. La segunda sección lista los eventos programados.

Figura 2.4. Pantalla para Añadir una Acción al Programador



Seleccione una Acción, una Hora y un Día, y pulse el botón Añadir para añadir un nuevo evento al programador. Esto moverá la entrada a la siguiente sección y la listará como activada.

Seleccione una Acción entre 'Reconectar', 'Conectar', 'Desconectar', 'Reiniciar', 'Apagar', 'Forzar actualización DynDNS', o 'Cambiar al Perfil'.

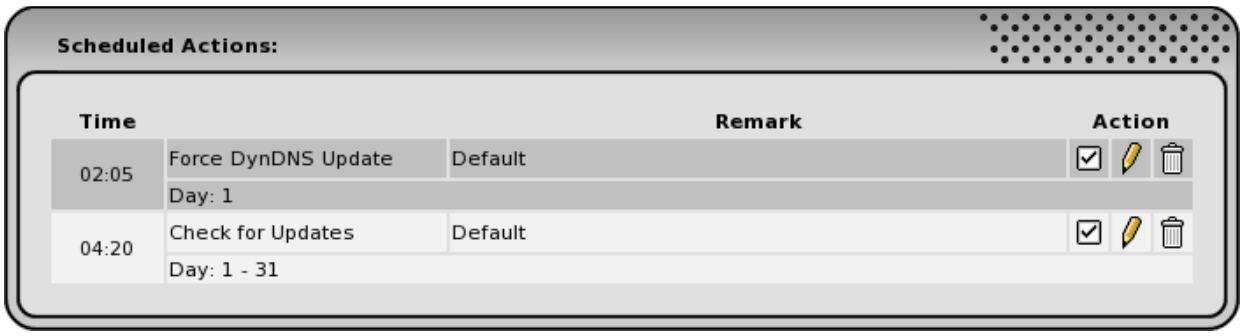
La opción para cambiar a un Perfil de Conexión diferente requiere la creación de Perfiles alternativos, que se configuran en la página Administración de marcado.

Las versiones más recientes también incluyen acciones para iniciar y parar IPsec VPN y el servidor OpenVPN, y puede programar comprobaciones de actualizaciones de Lista negra para URL Filter.

Opcionalmente, puede incluir una Descripción para describir el evento.

Hay un par de eventos por defecto, ya creados para usted, como puede ver más abajo.

Figura 2.5. Sección Acciones Programadas



La sección Acciones Programadas lista los eventos actuales. Para editar uno, pinche en el icono del *lápiz amarillo*. Los datos de la entrada se mostrarán en el formulario superior. Realice sus cambios y pulse el botón Actualizar en el formulario.

Para activar o desactivar una entrada, pinche en la casilla en la columna Acción del evento que quiere activar o desactivar. El icono cambia a una casilla vacía cuando la entrada está desactivada. Pinche en la casilla para activarla de nuevo.

Para borrar una entrada, pinche en su icono de la *papelera*.

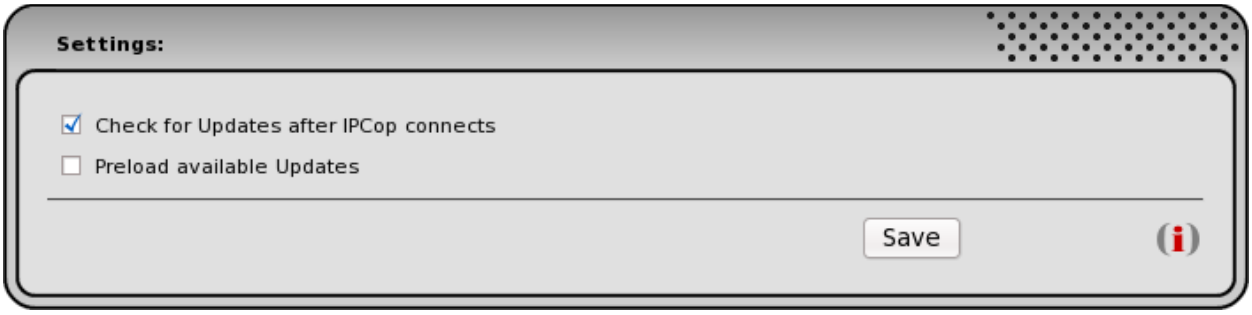
2.2.2. Actualizaciones

Esta página le permite descargar y aplicar actualizaciones y parches.

2.2.2.1. Ajustes

La primera sección le permite configurar comprobaciones automáticas de actualizaciones y si éstas se descargan en segundo plano.

Figura 2.6. Ajustes



Buscar actualizaciones cuando IPCop se conecte. Ahora es posible desactivar la 'Llamada a Casa' tras conectarse desmarcando esta casilla. Para desactivar por completo la llamada a casa, cualquier 'Comprobación de Actualizaciones' también debería eliminarse o ser desactivada.

Si la llamada a casa está desactivada, se recomienda encarecidamente la suscripción a la lista de correo ipcop-announce

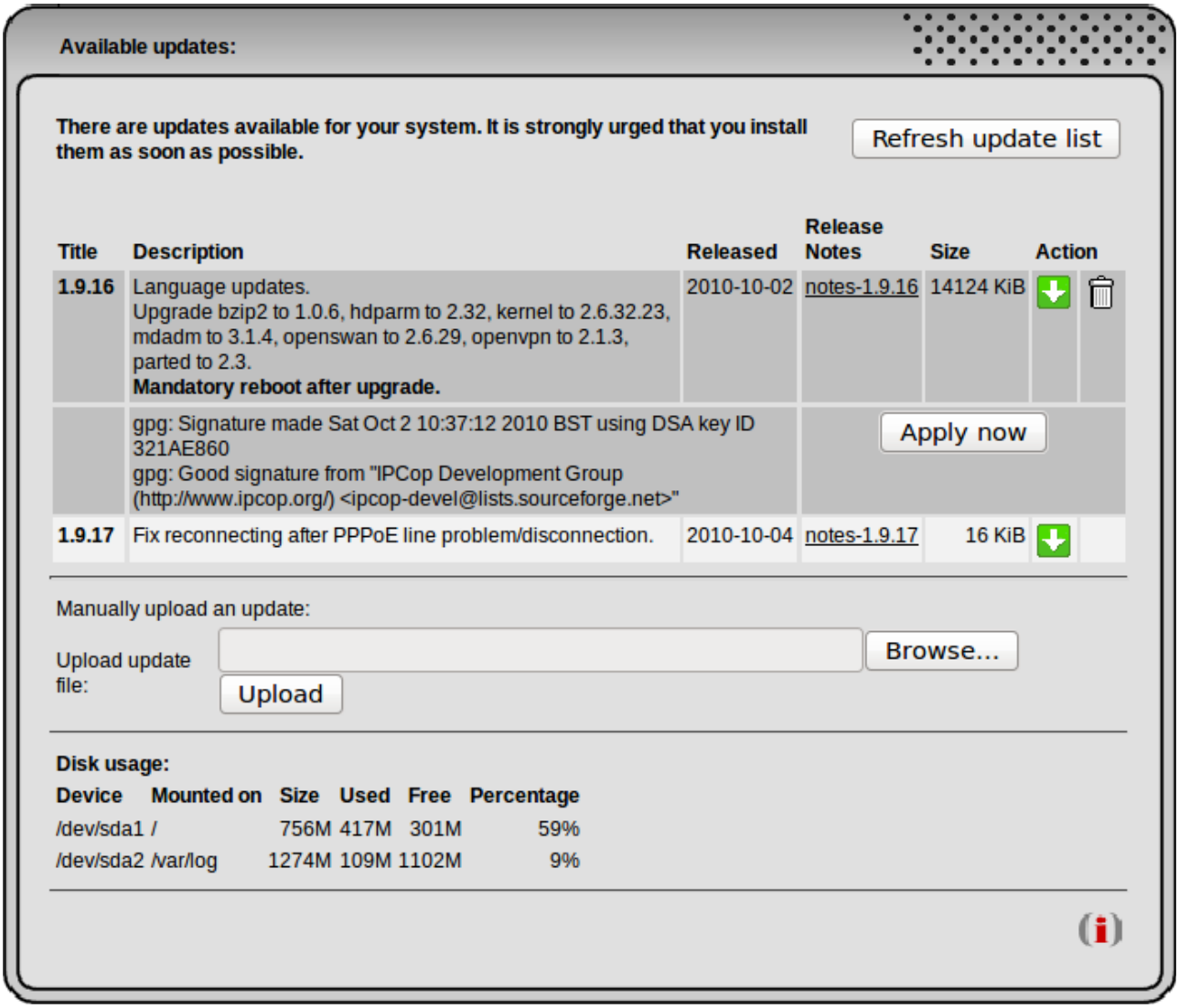
Precargar actualizaciones disponibles. Esto cargará (**¡no aplicará!**) actualizaciones cuando se detecten al 'Buscar actualizacones'.

Guardar. Para guardar sus ajustes, pulse el botón Guardar.

2.2.2.2. Actualizaciones disponibles

La segunda sección muestra una lista de las actualizaciones disponibles con enlaces para que pueda descargar las Notas y para descargar las actualizaciones directamente a IPCop.

Figura 2.7. Actualizaciones disponibles



Si está configurado en la sección superior, cada vez que se conecte a Internet, IPCop comprobará si hay alguna actualización disponible. También puede buscar actualizaciones manualmente pulsando el botón Refrescar lista de actualizaciones. Cuando esté diaponible una nueva actualización verá la información en pantalla, con una descripción y un botón para descargar el archivo de actualización.

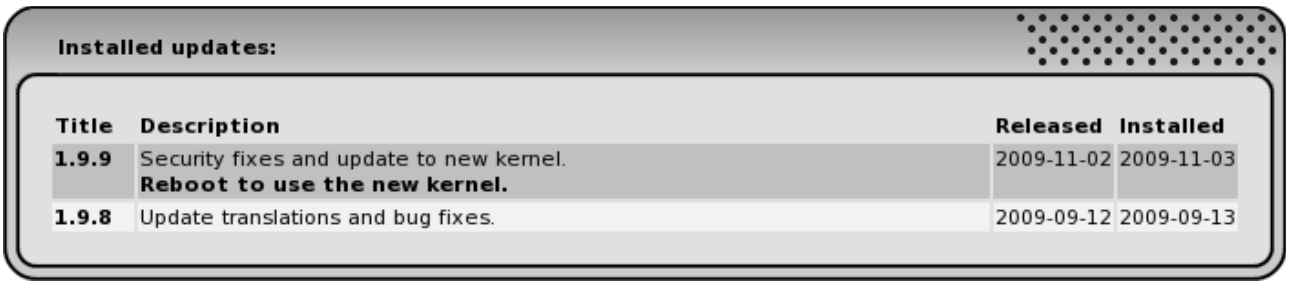
Pinchar el icono *Descargar* descargará el archivo `.tgz.gpg` directamente a su IPCop. Si la descarga es correcta, y la firma coincide, aparecerá el botón Aplicar ahora. Púlselo para aplicar la actualización.

El método alternativo, manual, requiere que usted descargue el archivo `.tgz.gpg` a su PC cliente con un navegador, no directamente a IPCop. Primero, localice el archivo de actualización en Sourceforge y descárguelo a su PC. Una vez que tenga el archivo, navegue hasta su localización en su PC usando el botón Buscar... en la sección Subir archivo de actualización. El botón Subir subirá el archivo a IPCop. Si la subida es correcta, y la firma coincide, aparecerá el botón Aplicar ahora. Púlselo para aplicar la actualización.

2.2.2.3. Actualizaciones instaladas

La tercera sección lista las actualizaciones que han sido instaladas.

Figura 2.8. Actualizaciones instaladas



Nota

Sólo los parches oficiales de IPCop (que han sido firmados con **gpg**) se instalarán en su IPCop. Algunas actualizaciones pueden requerir que reinicie su IPCop, así que, por favor, lea **toda** la información del parche cuidadosamente antes de aplicar la actualización.

Resolución de problemas

Si recibe un mensaje de error “Esta no es una actualización autorizada”, compruebe si el reloj de IPCop está en el pasado, ya que **gpg** pensará que la fecha de la firma está en el futuro, y se detendrá con un error.

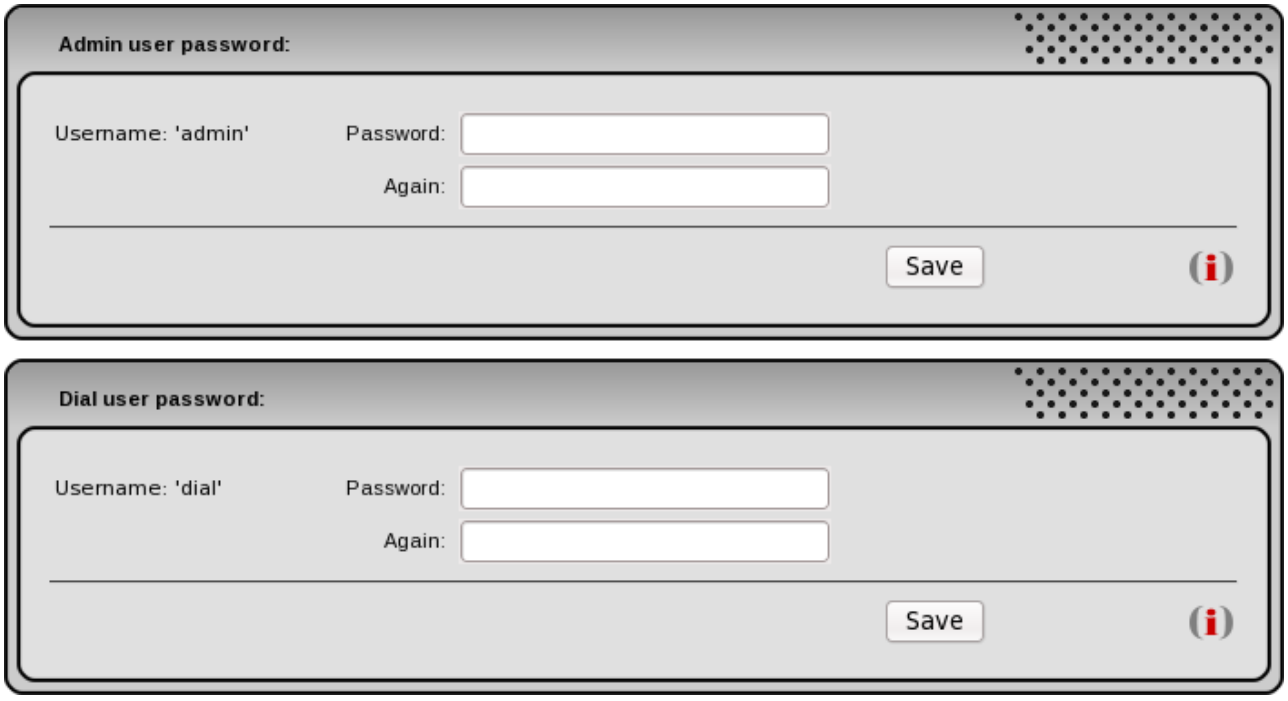
Revise el archivo de registro `/var/log/httpd/error_log` para confirmarlo.

IPCop es corrido a menudo en hardware antiguo, y la pila de la placa puede estar gastada, haciendo que el reloj del sistema falle.

2.2.3. Contraseñas

Esta página le permite cambiar las contraseñas de los usuarios 'admin' y/o 'dial'.

Figura 2.9. Pantalla de contraseñas



Introduzca la contraseña deseada una vez en cada campo para el usuario que quiere actualizar y pulse el botón Guardar.

Si introduce una contraseña para el usuario 'dial', se activará la ID de usuario 'dial'. Este usuario especial puede usar los botones Conectar y Desconectar en la pagina de Inicio, pero no puede acceder a ninguna otra página de IPCop. Utilice esta prestación si tiene una conexión por marcado y quiere que los usuarios se conecten a Internet, pero que no tengan autoridad administrativa en el cortafuegos.

Contraseñas de 'root' y 'backup'

Para cambiar la contraseña de 'root' o de 'backup' necesita volver a correr **setup** desde una consola.

Entre como 'root' y ejecute el comando:

```
$ setup
```

Seleccione `'Contraseñas'` del primer menú, y `Contraseña de 'root'` o `Contraseña de 'backup'` del siguiente menú e introduzca una contraseña.

La longitud mínima de una contraseña es de 6 caracteres.

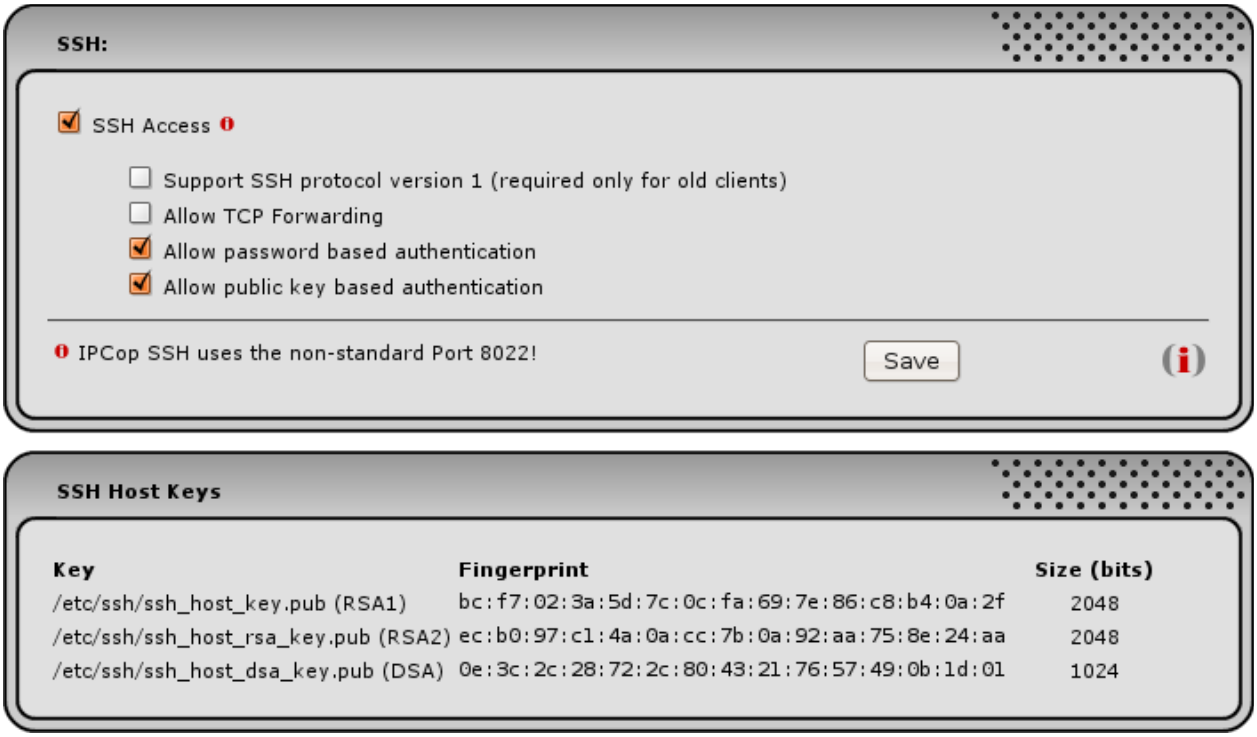
2.2.4. Acceso SSH

Esta página le permite decidir si el acceso remoto SSH está disponible en su IPCop o no. Marcando la casilla, activará el acceso remoto SSH. También es posible configurar varios parámetros del demonio SSH desde esta página. La opción SSH está desactivada por defecto y recomendamos que se active **sólo cuando se necesite y se desactive a continuación**.

Nota

Usando la página Ajustes del cortafuegos es posible configurar selectivamente qué redes pueden usar el acceso remoto SSH.

Figura 2.10. Acceso SSH y claves SSH del host



Así como el puerto HTTPS para la interfaz GUI de IPCop ha cambiado al puerto 8443, el puerto SSH para acceso SSH a IPCop ha cambiado al 8022. Si está usando una aplicación GUI para acceder a su IPCop, recuerde especificar el puerto 8022.

Cambiar el puerto SSH

La utilidad de línea de comandos **setreservedports** está disponible para permitir a los administradores cambiar el puerto seguro. Vea la sección sobre setreservedports para más detalles.

Si está usando comandos ssh, scp o sftp, la sintaxis para especificar puertos no estándar es diferente para cada comando, incluso aunque todos ellos están relacionados. Asumiendo que su IPCop está en la dirección 192.168.254.1, los comandos serían:

SSH

```
$ ssh -p 8022 root@192.168.254.1
```

SCP a IPCop

```
$ scp -P 8022 algun/archivo root@192.168.254.1:
```

SCP desde IPCop

```
$ scp -P 8022 root@192.168.254.1:/ruta/a/algun/archivo ruta/a/copia/local
```

SFTP

```
$ sftp -o port=8022 root@192.168.254.1
```

Use las páginas 'man' de su máquina de escritorio para encontrar una explicación más completa de estos comandos.

2.2.4.1. Opciones de SSH

Las siguientes opciones de SSH están disponibles desde la página web:

Acceso SSH

Marcar esta casilla activa SSH. A menos que use acceso externo, SSH sólo estará disponible desde la red VERDE. Con SSH activado es posible para cualquiera con la contraseña de 'root' de IPCop entrar a su cortafuegos a la línea de comandos.

Soportar protocolo SSH versión 1 (requerido sólo para clientes antiguos)

Marcar esta casilla activa el soporte para los clientes SSH de versión 1. El uso de esta opción está completamente desaconsejado. Hay vulnerabilidades conocidas en la versión 1 de SSH. Use esta opción sólo para acceso temporal si sólo tiene clientes con versión 1 y no hay manera de actualizarlos a SSH versión 2. La mayoría de los clientes SSH actuales, si no todos, soportan la versión 2. Actualice sus clientes en cuanto sea posible.

Permitir reenvío TCP

Marcar esta casilla, le permite crear túneles SSH encriptados entre máquinas detrás de su cortafuegos y usuarios externos.

¿Qué utilidad tiene esto si IPCop ya tiene una VPN?

Está fuera y algo va mal en uno de sus servidores. No ha configurado una conexión VPN 'roadwarrior'. Si conoce la contraseña de 'root' de su IPCop puede usar el reenvío de puertos SSH para pasar a través de su cortafuegos y tener acceso al servidor que está en una de sus redes protegidas. Los siguientes párrafos tratarán acerca de cómo hacer esto, asumiendo que tiene un servidor Telnet corriendo en un ordenador interno en 10.0.0.20. También se asume que su máquina remota es una máquina Linux. La aplicación Putty para Windows tiene las mismas posibilidades, pero se utilizan mediante diálogos. Puede que ya haya realizado uno o más de los dos primeros pasos.

1. Active o haga que alguien active el acceso externo al puerto 8443, el puerto HTTPS.
2. Use las páginas web de su IPCop para activar el acceso SSH y el acceso externo al puerto 8022.
3. Cree un túnel SSH entre su máquina remota y el servidor interno que está corriendo un demonio SSH ejecutando el comando:
4. `$ ssh -p 8022 -N -f -L 12345:10.0.0.20:23 root@ipcop`
   -p 8022

IPCop escucha SSH en el puerto 8022, no el habitual 22.

-N

en conjunción con -f, le dice a SSH que corra en segundo plano sin cerrarse. Si usa esta opción, deberá recordar que tiene que usar 'kill' para terminar el proceso SSH. Como alternativa, puede añadir el comando **`sleep 100`** al final de la línea y no usar la opción -N. Si hace esto, el SSH invocado por el comando ssh terminará después de 100 segundos, pero la sesión telnet y su túnel no terminarán.

-f

opción para correr SSH en segundo plano.

-L

le dice a SSH que construya un túnel de reenvío de puerto como se especifica con los siguientes parámetros.

12345

El puerto local que se usará para tunelar el servicio remoto. Éste debe ser mayor de 1021, o de lo contrario deberá estar actuando como 'root' para enlazarse a puertos conocidos.

10.0.0.20

Esta es la dirección VERDE del servidor remoto.

23

Esto especifica el número de puerto remoto a usar, Telnet.

root@ipcop.fqn

Finalmente, esto especifica que estará usando su cortafuegos IPCop como el agente de reenvío de puertos. Necesitará una ID de usuario para acceder, y la única disponible en IPCop es 'root'. Se le preguntará la contraseña de 'root' para IPCop.

5. Por último, acceda al Telnet remoto usando el túnel.
6. `$ telnet localhost 12345`

   localhost es la máquina en la que está trabajando. La dirección de 'loopback' 127.0.0.1 está definida como 'localhost'. 12345 es el puerto local del túnel especificado en el comando anterior.

Hay un tutorial sobre el reenvío de puertos mediante SSH en Dev Shed.

Permitir autenticación basada en contraseñas

Permite a los usuarios acceder a IPCop usando la contraseña de 'root'. Si decide desactivar esto, cree sus claves SSH primero, y verifique que puede acceder usando los archivos de claves.

Permitir autenticación basada en clave pública

Marcando esta casilla, se podrá utilizar la autenticación mediante clave pública para SSH. Este es el mejor método de asegurar IPCop cuando se usa SSH. Este artículo tiene un debate acerca del uso de **SSH-keygen** para generar claves RSA y cómo usarlas con SSH.

2.2.4.2. Claves de host SSH

Esta sección lista las huellas de la clave de host usada por SSH en IPCop para verificar que está abriendo una sesión con la máquina correcta. La primera vez que se abre una sesión, se mostrará una de las huellas en SSH y se le preguntará si es correcta. Si lo desea, puede verificarla mirando en esta página.

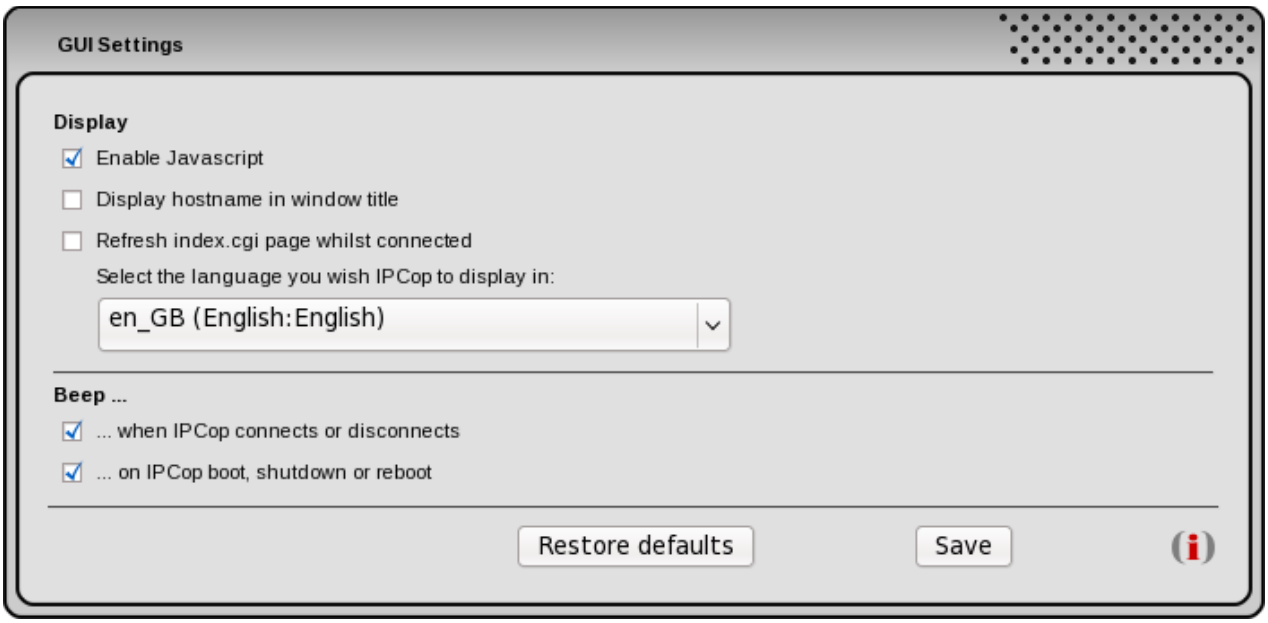
2.2.5. Ajustes de GUI

Esta página controla la apariencia y funcionalidad de las páginas web de IPCop.

Tras realizar cualquier cambio, recuerde pulsar el botón Guardar.

Para restaurar los valores por defecto, pulse el botón Restaurar valores por defecto, y pulse el botón Guardar.

Figura 2.11. Ajustes de GUI



2.2.5.1. Apariencia

Activar Javascript. Las páginas web administrativas usan abundante JavaScript para proporcionar una apariencia mejorada. De todas formas, algunos navegadores no funcionan bien con JavaScript. Si esta casilla no está marcada, los diferentes menús desplegables estarán desactivados y sus opciones en cualquier página aparecerán a lo ancho en la parte superior de la página.

Mostrar nombre de host en el título de la ventana. Esta casilla hará que se muestre el nombre de host de IPCop en la parte superior de cada página. Si está manteniendo más de un IPCop, esto puede ser de ayuda, ya que podrá saber qué IPCop está mostrando su navegador en cada momento.

Refrescar la página index.cgi mientras esté conectado. Por defecto, la página de inicio se refresca una vez cuando IPCop se conecta a Internet, y pulsar manualmente el botón “Refrescar” fuerza a la página de inicio a actualizarse con el último tiempo de conexión.

Activar esta opción fuerza a la página de inicio a refrescarse cada 30 segundos, por lo que el tiempo de conexión se actualiza regularmente, y si la conexión se cae por falta de actividad, aparecerá el mensaje de estado “Marcado bajo demanda en espera”.

Seleccione el idioma en el que desea que se muestre IPCop. Este menú desplegable le permitirá elegir cuál de los 34 idiomas actualmente disponibles para las páginas de IPCop, usará su IPCop para mostrarlas.

Nota

Cuando una traducción de idioma está sólo parcialmente completada, se usa la frase en inglés en su lugar.

Si quiere añadir o mejorar una traducción existente, por favor, considere unirse a uno de los equipos de traducción listados en la página Créditos del sistema, y contacte con los desarrolladores de IPCop (ver más abajo).

También puede seleccionar el idioma a usar por IPCop durante la instalación. De todas formas, su idioma deseado puede no estar disponible durante la instalación. El grupo de traducción de IPCop está planeando hacer disponibles más idiomas en función de la ayuda de los voluntarios al esfuerzo

de traducción. Cuando los nuevos idiomas estén disponibles, se añadirán mediante el sistema regular de actualizaciones.

Por supuesto, puede desear traducir IPCop a otro idioma usted mismo. Si es así, le pedimos que contacte con los desarrolladores de IPCop en la lista de correo ipcop-devel. Por favor, consulte la página IPCop How To Translate para más detalles.

2.2.5.2. Sonido

Pitar cuando IPCop se conecta o desconecta. Por defecto, IPCop pitará cuando la conexión a Internet se "levante" o se "caiga".

Desactive esta opción para un funcionamiento silencioso.

Pitar cuando IPCop arranca, se apaga o se reinicia. Por defecto, IPCop pitará cuando complete el arranque, y pitará cuando complete el apagado.

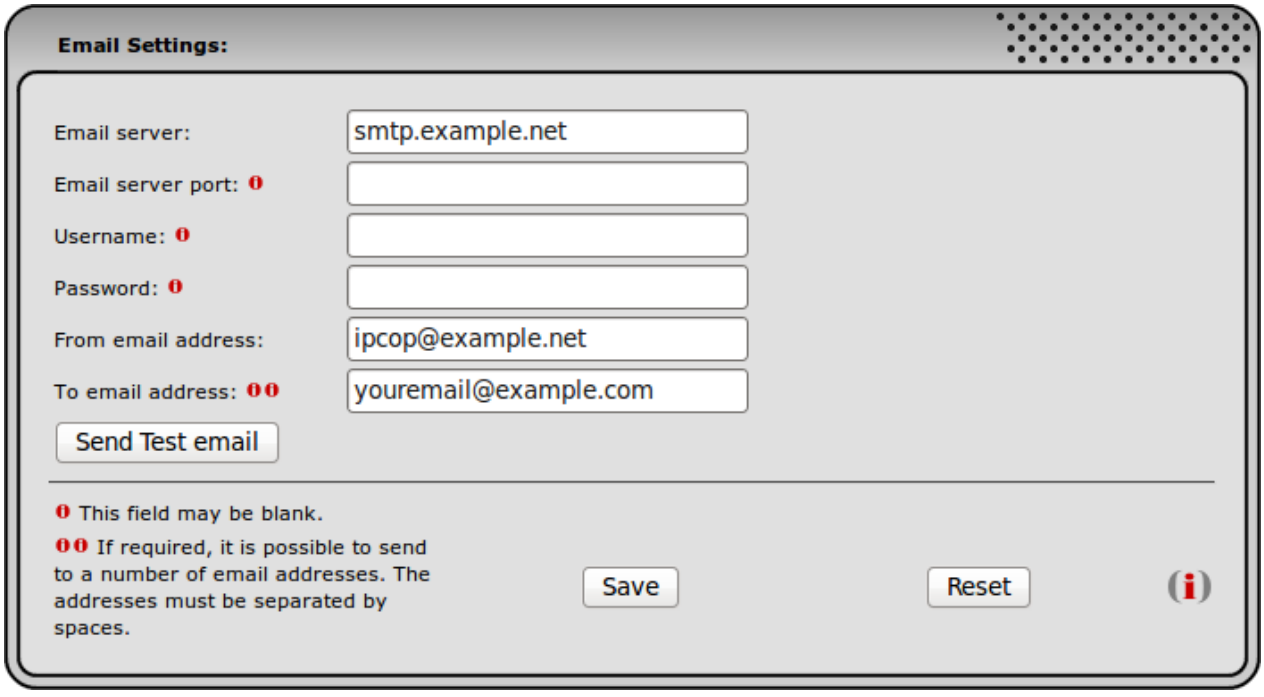
Desactive esta opción para arranques y apagados silenciosos.

2.2.6. Ajustes de correo

Esta página controla la funcionalidad de correo de IPCop. IPCop es capaz de enviarle correos en determinadas situaciones o eventos, como por ejemplo si se ha excedido un volumen de tráfico monitorizado.

Tras realizar cualquier cambio, recuerde pulsar el botón Guardar.

Figura 2.12. Ajustes de correo



Servidor de correo. Introduzca la dirección de su servidor de correo aquí. Por ejemplo: `smtp.ejemplo.net`

Puerto del servidor de correo - opcional. Si su servidor de correo usa un puerto no estándar para las conexiones, introdúzcalo aquí. De lo contrario, déjelo en blanco.

Nombre de usuario - opcional. Si su servidor de correo requiere un nombre de usuario para la cuenta de correo, introdúzcalo aquí. De lo contrario, déjelo en blanco.

Contraseña - opcional. Si su servidor de correo requiere una contraseña para la cuenta de correo, introdúzcala aquí. De lo contrario, déjelo en blanco. Observe que usar espacios o comillas simples o dobles (' ") en la contraseña causará un error.

Dirección de origen. Introduzca la dirección de correo que enviará los correos. Aparecerá como dirección "De" cuando reciba correos de IPCop.

Dirección de destino. Introduzca su dirección de correo, o la dirección de correo a la que quiere enviar los mensajes en este campo.

Es posible enviar un correo a varias direcciones. Introduzca las direcciones en este campo, separadas por espacios.

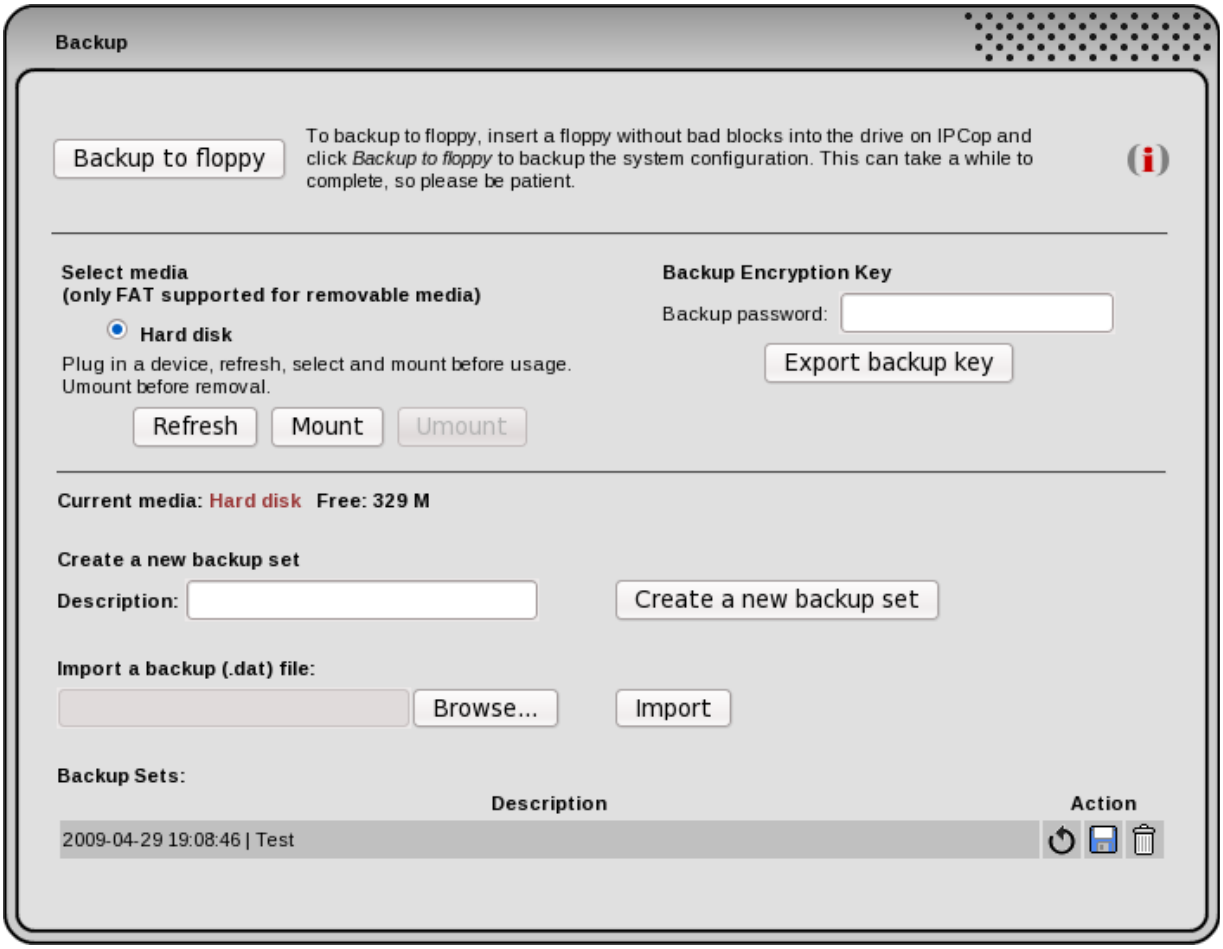
Enviar correo de prueba. Envía un mensaje para comprobar si IPCop puede enviar correo con los ajustes proporcionados.

Necesita Guardar los ajustes primero, antes de intentar envíar un correo de prueba.

2.2.7. Página de copia de seguridad

Esta página le permite hacer copias de seguridad de los ajustes de su sistema tanto a disquete (si tiene uno instalado) como a un archivo. Los archivos se pueden guardar en el disco duro, o en una memoria USB, y se pueden exportar y restaurar desde esta página.

Figura 2.13. Pantalla de copias de seguridad



2.2.7.1. Copia a disquete

La sección superior del panel de la página de copias de seguridad le permite copiar la configuración de su IPCop a un disquete. La única manera de restaurar su configuración desde un disquete es reinstalar el sistema desde un CD-Rom o HTTP/FTP. Al principio del proceso de instalación se le preguntará si tiene un disquete con la configuración de IPCop en él. Su configuración será restaurada y la instalación terminará.

Ponga un disquete en el lector y pulse el botón Copiar a disquete. Su configuración será escrita al disquete y verificada.

Todos los mensajes de error y cualquier información generada durante una copia de seguridad aparecerá en el pie del panel.

2.2.7.2. Copia a archivo

El resto del panel le permite crear múltiples conjuntos de copias de seguridad y seleccionar diferentes medios en los que guardar los archivos. Por defecto es el disco duro de IPCop, pero las memorias USB están soportadas.

Por seguridad, las copias de seguridad creadas en la página de Copias de seguridad, están encriptadas usando su contraseña de 'backup'. Para asegurarse, introduzca la contraseña de 'backup' y exporte la clave usando el botón proporcionado, además de exportar sus copias de seguridad. Necesitará la clave de 'backup' si quiere instalar desde una memoria USB o si necesita restaurar los ajustes tras un fallo de disco duro.

Para importar una copia de seguridad durante la instalación de IPCop, se le preguntará por la clave de 'backup'.

2.2.7.3. Clave de encriptación de 'backup'

Para usar la prestación de exportación de la clave de 'backup' haga lo siguiente:

1. Ponga una contraseña para 'backup'.
2. En la página de Copias de seguridad escriba esta contraseña en el campo apropiado. La clave se exporta encriptada y tendrá que elegir dónde escribir el archivo cuando pulse el botón Exportar clave de 'backup'.
3. Cree una copia de seguridad y exporte el archivo `.dat` (no necesita rellenar el campo contraseña de 'backup' esta vez).

   Ahora tiene todo lo que necesita para poder instalar la configuración de un sistema desde una memoria USB o un servidor http/ftp.
4. Escriba el archivo `.dat`, sin la marca de tiempo en el nombre y el archivo de clave encriptado en el medio que desee utilizar para restaurar (memoria USB o servidor http/ftp), y la restauración funcionará si introduce la contraseña de 'backup' correcta y el nombre de host coincide con la clave encriptada y el nombre del archivo .dat.

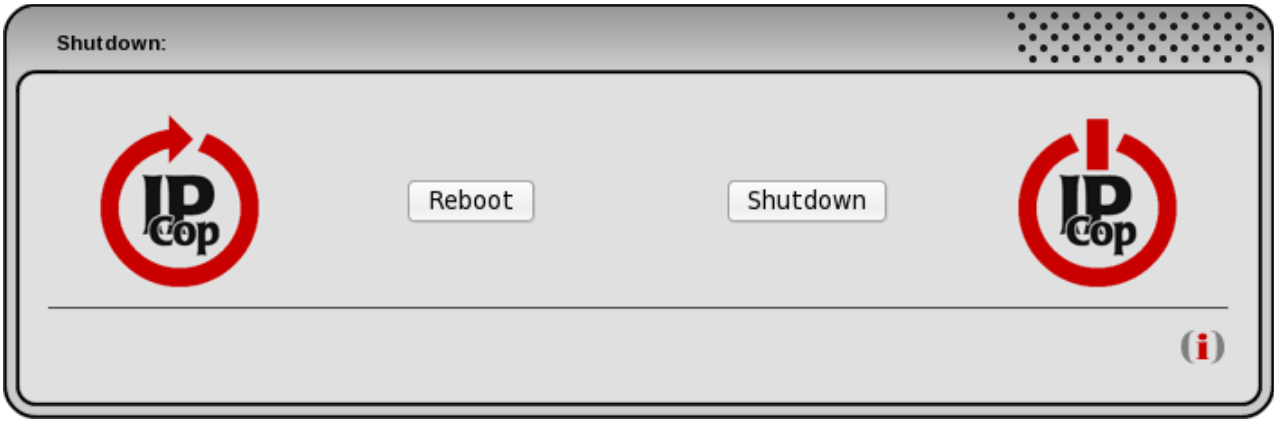
Nota

Cuando use una memoria USB, puede emplear archivo(s) `.dat` con marca de tiempo. IPCop buscará primero un archivo `.dat` sin la marca de tiempo, y si no lo encuentra, usará el archivo `.dat` con la marca de tiempo más reciente para la restauración.

2.2.8. Página Apagar

Esta página le permite tanto Apagar como Reiniciar IPCop. Simplemente, pulse el botón para la opción que desee.

Figura 2.14. Apagar



2.2.8.1. Reiniciar o apagar

Pulse uno de los botones Reiniciar o Apagar para reiniciar o parar IPCop *inmediatamente*.

Sugerencia

También puede apagar su IPCop pulsando el botón de encendido/apagado (asumiendo que su hardware soporte esta característica).

2.3. Menú Estado

Este grupo de páginas le ofrece información y estadísticas de IPCop. Para llegar a estas páginas, seleccione Estado en la barra de pestañas de la parte superior de la pantalla. Aparecerán las siguientes opciones en un menú desplegable:

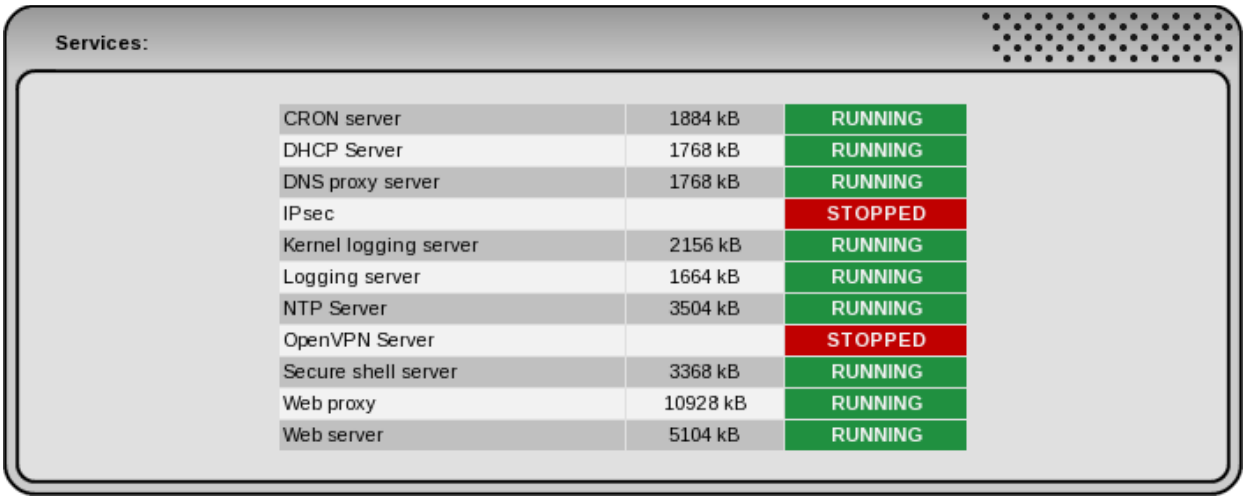
- Estado del Sistema
- Información del Sistema
- Estado de la Red
- Gráficos del Sistema
- Gráficos de Tráfico
- Gráficos del Proxy
- Recuento de Tráfico
- Conexiones
- IPTables

2.3.1. Estado del Sistema

Las páginas de Estado le presentan una lista de información MUY detallada acerca del estado actual de su IPCop. La primera página, Estado del Sistema, muestra lo siguiente, en orden de arriba hacia abajo:

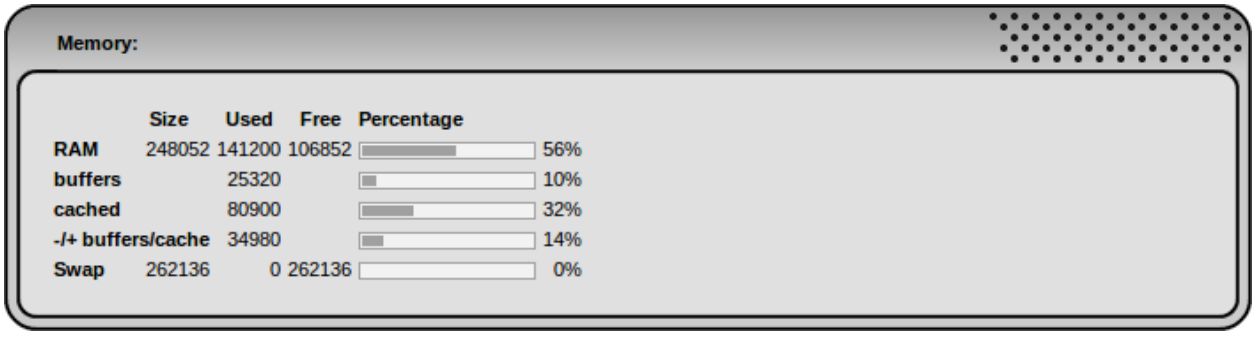
2.3.1.1. Servicios

Servicios - Muestra qué servicios están corriendo actualmente y la memoria usada.



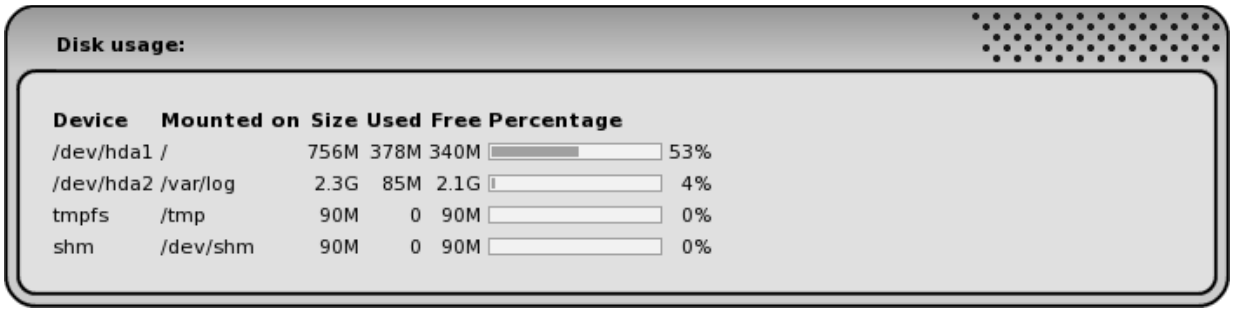
2.3.1.2. Memoria

Memoria - Muestra el uso de memoria/intercambio en su IPCop.



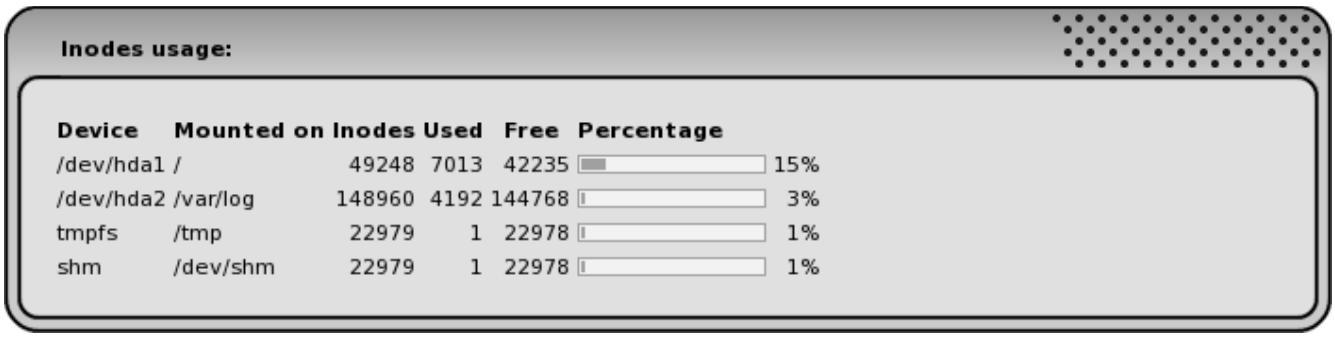
2.3.1.3. Uso de disco

Uso de disco - Muestra la cantidad de disco total/usada/libre del espacio en disco de su IPCop.



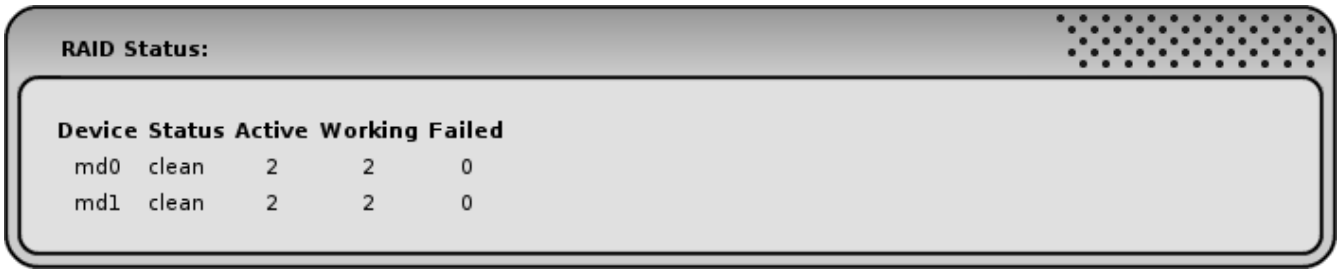
2.3.1.4. Uso de inodos

Uso de inodos - Esto muestra el número total/usados/libres de inodos en su IPCop.



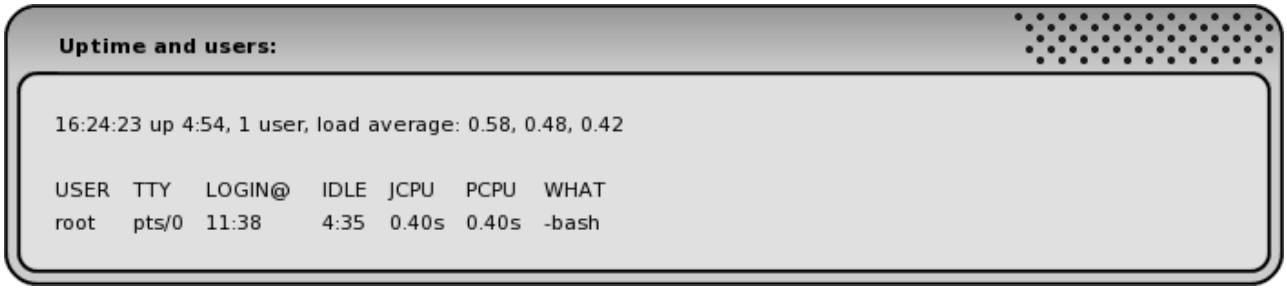
2.3.1.5. Estado del RAID(específico del sistema)

Estado del RAID - Esto muestra información de los dispositivos RAID en su IPCop, si existen.



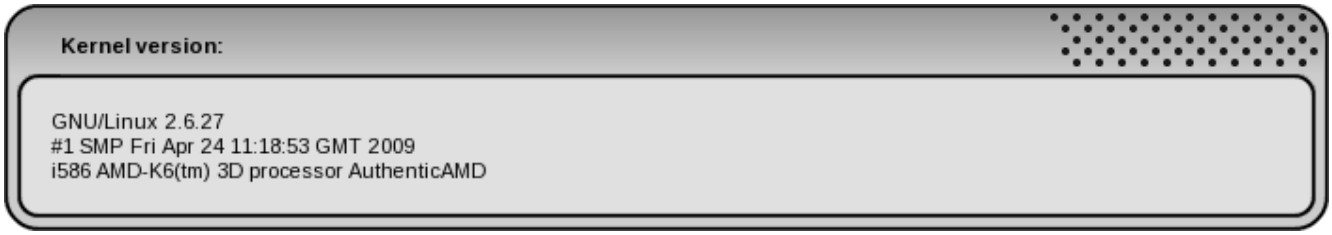
2.3.1.6. Tiempo de actividad y usuarios

Tiempo de actividad y usuarios - Muestra la salida del comando **w**, que muestra el tiempo de actividad e información de los usuarios actualmente logeados en su IPCop.



2.3.1.7. Versión del Núcleo

Versión del Núcleo - Esto muestra información sobre el propio Núcleo de IPCop.



2.3.2. Información del Sistema

Esta página muestra información sobre el hardware y los dispositivos de su IPCop.

2.3.2.1. Información de CPU

Información de CPU - Esta sección muestra información de la CPU de su IPCop, como el fabricante, modelo, frecuencia de trabajo, tamaño de caché, etc.

2.3.2.2. Información del Cobalt (específico del sistema)

Esta sección sólo será visible si está corriendo IPCop en hardware Cobalt.

Información del Cobalt - Muestra información del hardware Cobalt de su IPCop, como la temperatura de la CPU, información de los slots de RAM, tipo de sistema, etc.

2.3.2.3. Disco del Sistema

Disco del Sistema - Esta sección muestra información como el fabricante, modelo, configuración y capacidades del disco de IPCop.

2.3.2.4. Dispositivos PCI

Dispositivos PCI - Esta sección muestra información acerca de los dispositivos PCI conectados a su IPCop.

2.3.2.5. Tarjetas de red

Tarjetas de red - Esta sección muestra información acerca de las tarjetas de red de su IPCop.

2.3.2.6. Estado de enlaces

Estado de enlaces - Esta sección muestra información sobre los enlaces LAN y WAN de su IPCop.

2.3.2.7. Dispositivos USB

Dispositivos USB - Esta sección muestra información sobre los dispositivos USB conectados a su IPCop.

2.3.2.8. Interrupciones usadas

Interrupciones usadas - Esta sección muestra las interrupciones usadas en su IPCop.

2.3.2.9. Estado de procesos

Estado de procesos - Esta sección muestra los procesos corriendo en su IPCop.

2.3.2.10. Módulos cargados

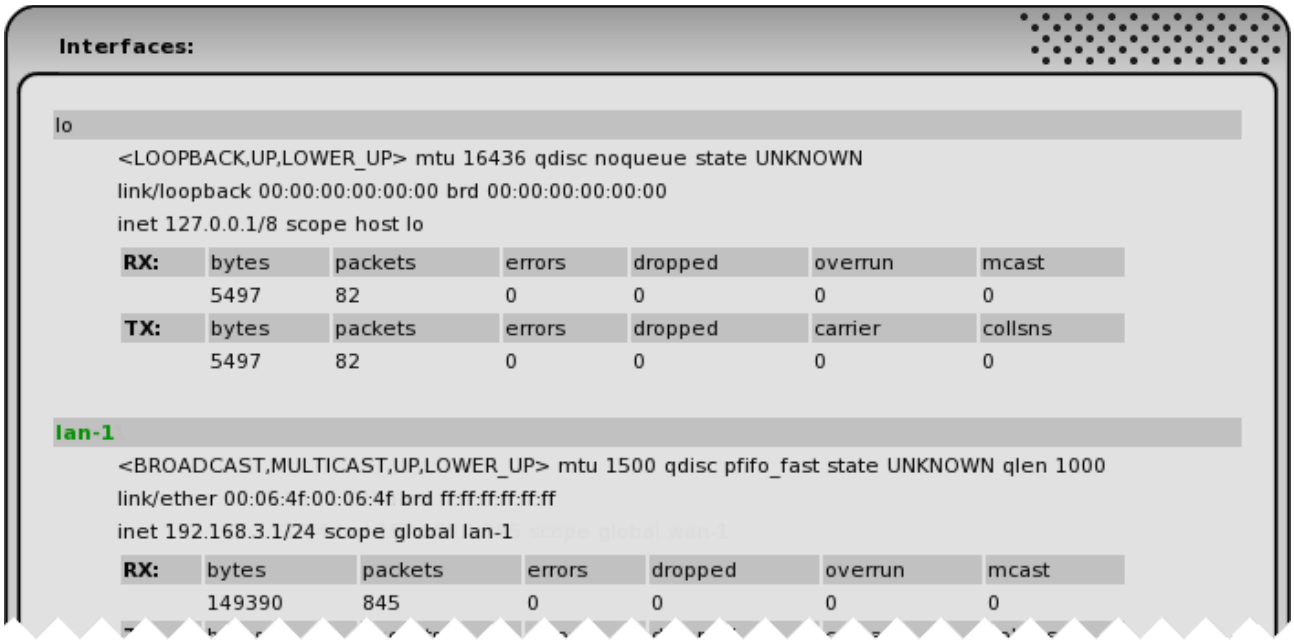
Módulos cargados - Esta sección lista los módulos cargados en su IPCop.

2.3.3. Estado de la red

Esta página muestra información acerca de las interfaces de red y de la configuración de red de su IPCop.

2.3.3.1. Interfaces

Interfaces - Esta sección muestra información acerca de *todos* sus dispositivos de red. Esto incluye PPP, IPSec, Loopback, etc.

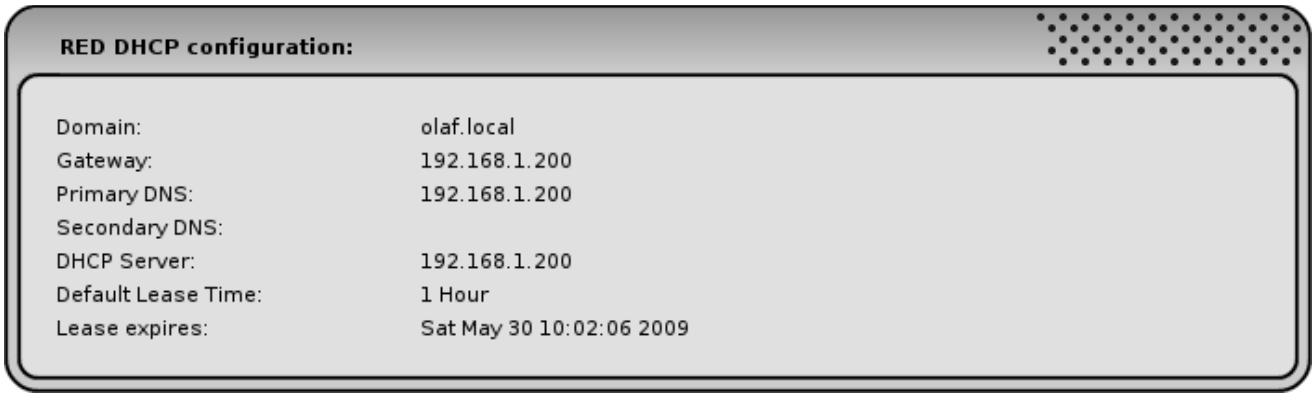


2.3.3.2. Configuración DNS Roja

Muestra el/los servidor(es) en uso.

2.3.3.3. Estado del cliente DHCP

Muestra el estado del cliente DHCP si su interfaz ROJA se configura con DHCP. Se muestran la puerta de enlace, servidor(es) DNS, dirección IP del servidor DNS, tiempo de concesión y tiempo de expiración de la concesión.

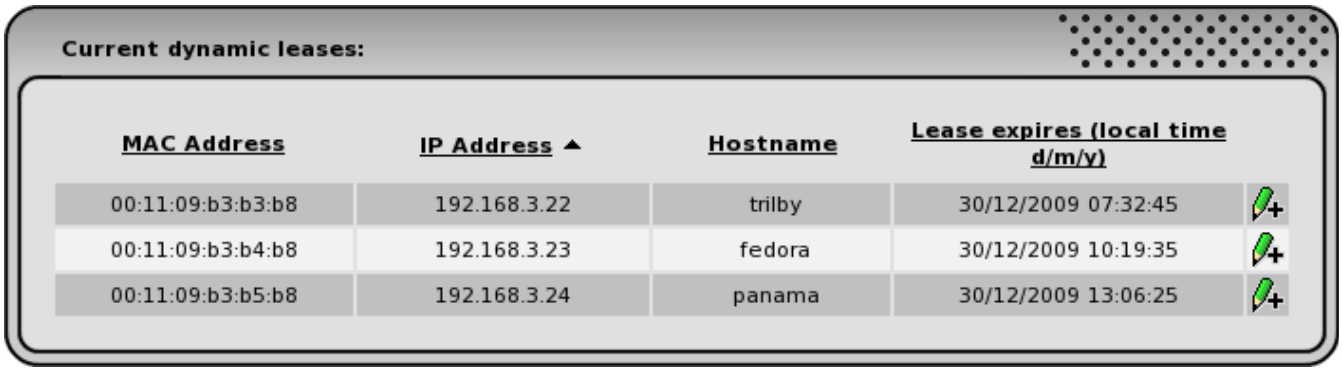


Nota

Esta sección *sólo* será visible si su interfaz ROJA se configura mediante DHCP.

2.3.3.4. Concesiones dinámicas actuales

Muestra el contenido del archivo `/var/run/dnsmasq/dnsmasq.leases` si está activado el servidor DHCP. Se listan las concesiones con el nombre de host si está disponible y el tiempo de expiración.



Current dynamic leases:

MAC Address	IP Address ▲	Hostname	Lease expires (local time d/m/y)
00:11:09:b3:b3:b8	192.168.3.22	trilby	30/12/2009 07:32:45
00:11:09:b3:b4:b8	192.168.3.23	fedora	30/12/2009 10:19:35
00:11:09:b3:b5:b8	192.168.3.24	panama	30/12/2009 13:06:25

Nota

Esta sección *sólo* será visible si está activado el servidor DHCP. Vea la sección Servidor DHCP para más detalles.

2.3.3.5. Configuración de ADSL

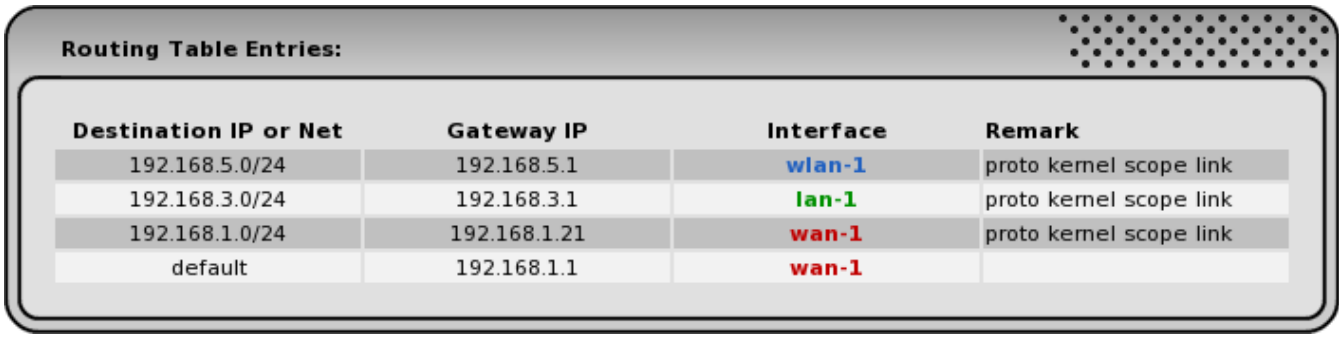
Muestra información acerca del dispositivo ADSL, si está presente.

Nota

Esta sección *sólo* será visible si hay un módem ADSL configurado.

2.3.3.6. Entradas de la tabla de enrutamiento

Muestra la tabla de enrutamiento actual y la puerta de enlace por defecto.

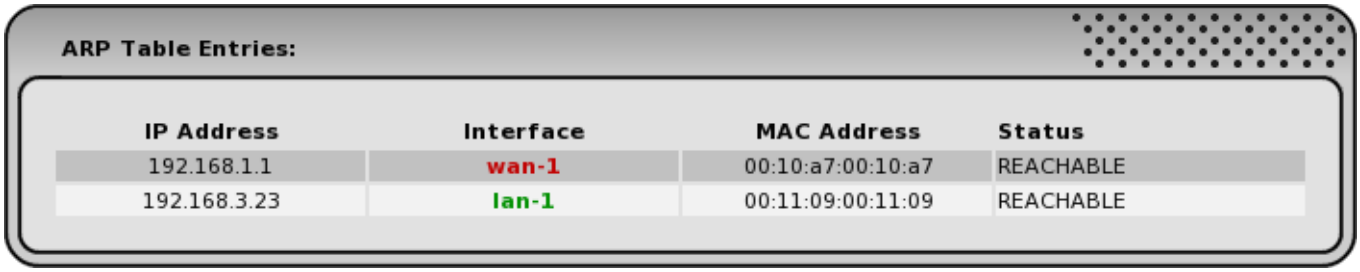


Routing Table Entries:

Destination IP or Net	Gateway IP	Interface	Remark
192.168.5.0/24	192.168.5.1	wlan-1	proto kernel scope link
192.168.3.0/24	192.168.3.1	lan-1	proto kernel scope link
192.168.1.0/24	192.168.1.21	wan-1	proto kernel scope link
default	192.168.1.1	wan-1	

2.3.3.7. Entradas de la tabla ARP

Muestra el contenido actual de la tabla ARP.



ARP Table Entries:

IP Address	Interface	MAC Address	Status
192.168.1.1	wan-1	00:10:a7:00:10:a7	REACHABLE
192.168.3.23	lan-1	00:11:09:00:11:09	REACHABLE

2.3.4. Gráficos del Sistema

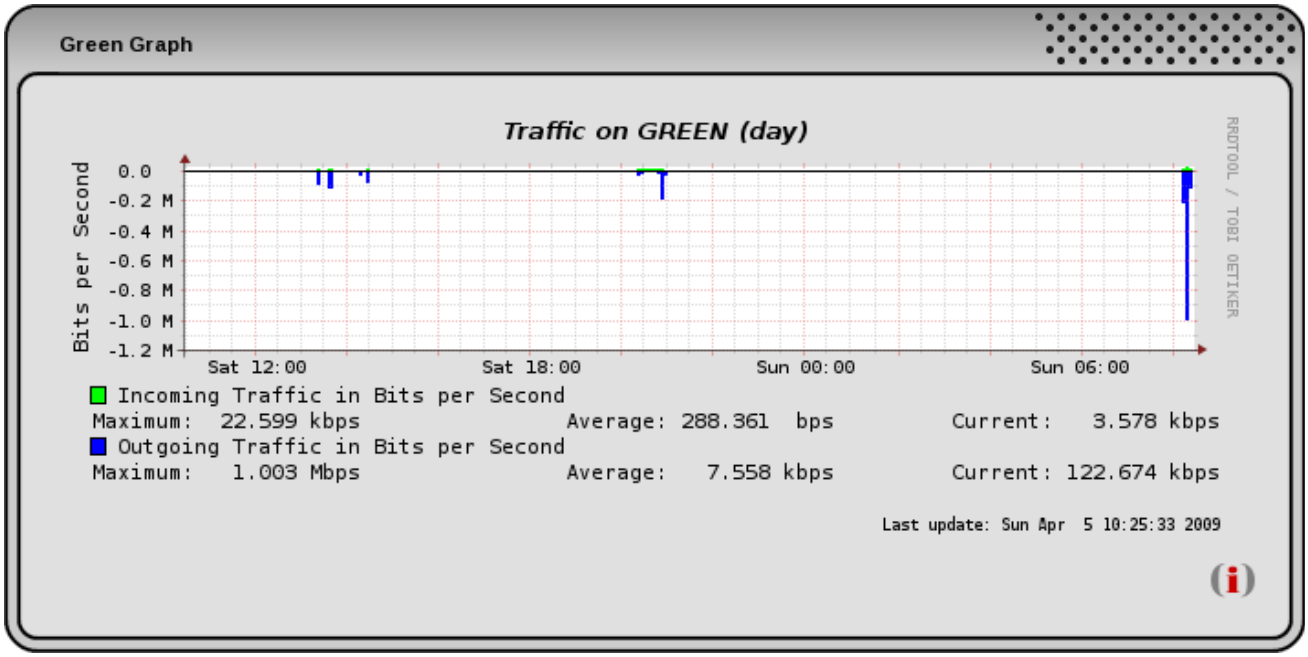
Esta página ilustra de forma gráfica el rendimiento de algunos de los sistemas de IPCop.

Hay secciones para el uso de CPU, uso de memoria, uso de disco y acceso a disco.

Pinche en uno de los gráficos para mostrar gráficos adicionales de uso por día, semana, mes y año.

2.3.5. Gráficos de Tráfico

Esta página ilustra de forma gráfica el tráfico de entrada y salida de IPCop.



Hay secciones para cada interfaz de red, Roja y Verde, (y Azul y Naranja si están configuradas) que muestran gráficos del tráfico entrante y saliente a través de esa interfaz.

Pinche en uno de los gráficos para mostrar gráficos adicionales del tráfico en esa interfaz por día, semana, mes y año.

¿Los gráficos de tráfico no funcionan?

Los gráficos se generan mediante un script, corrido cada cinco minutos por un 'cron job'. Si los gráficos están inesperadamente vacíos, compruebe que la hora es correcta y revise la página de 'cron' de los Registros del Sistema para ver si el script makegraphs se ejecuta cada cinco minutos. Si no lo hace, pruebe a reiniciar 'fcron' accediendo como usuario 'root' y ejecutando el comando **fcrontab -z**

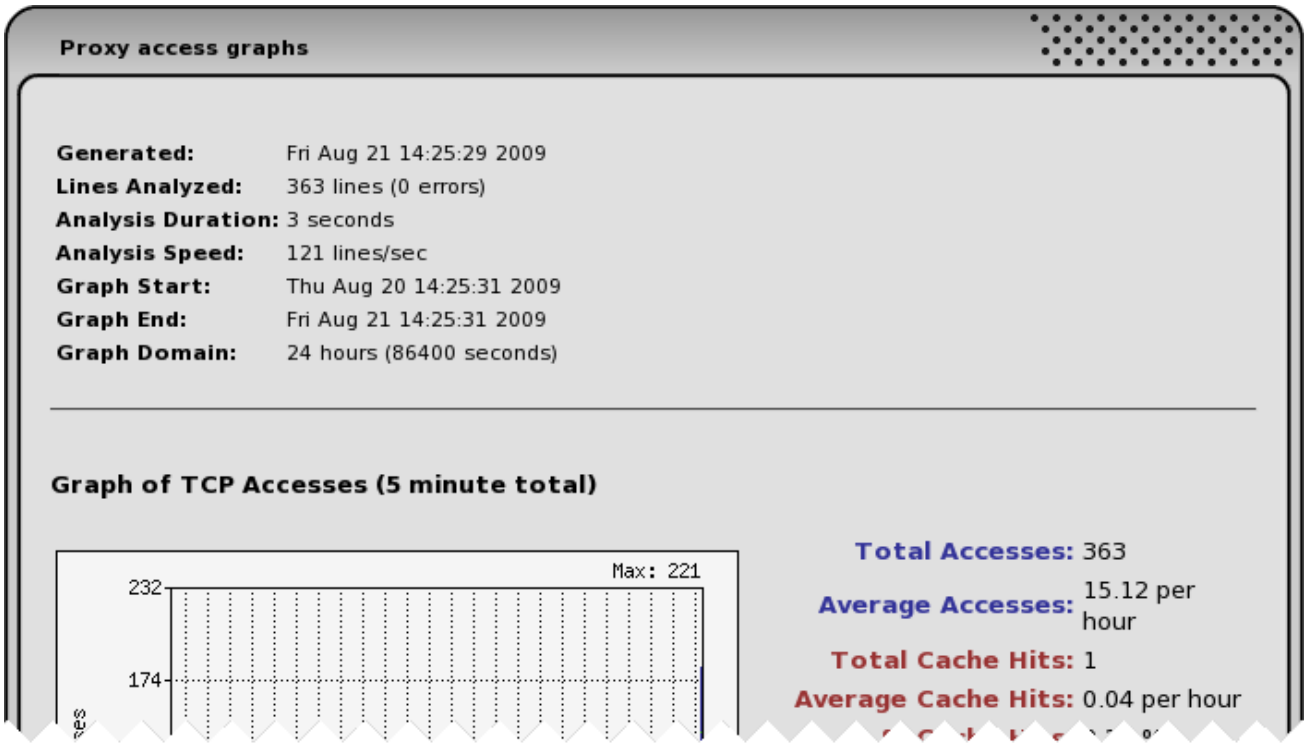
O ejecute manualmente el script makegraphs para ver si hay algún mensaje de error. Acceda a una consola como 'root' y ejecute el comando **makegraphs**

Si ha habido un cambio grande en el reloj de IPCop, especialmente hacia atrás, los archivos de la RRD (Round Robin Database) pueden no aceptar la hora. En este caso, debería considerar borrar los archivos de la base de datos, que puede encontrar en en directorio `/var/log/rrd`. Los archivos

de la base de datos se volverán a crear la próxima vez que se ejecute el script makegraphs, pero se perderán los datos anteriores.

2.3.6. Gráficos del Proxy

Esta página muestra la salida del comando **squid-graph**.



Nota

El registro **debe** estar activado en la página de administración del Proxy Web, o los gráficos estarán vacíos.

2.3.7. Recuento de Tráfico

El recuento de tráfico, cuando está activo, cuenta el tráfico en todas las interfaces configuradas.

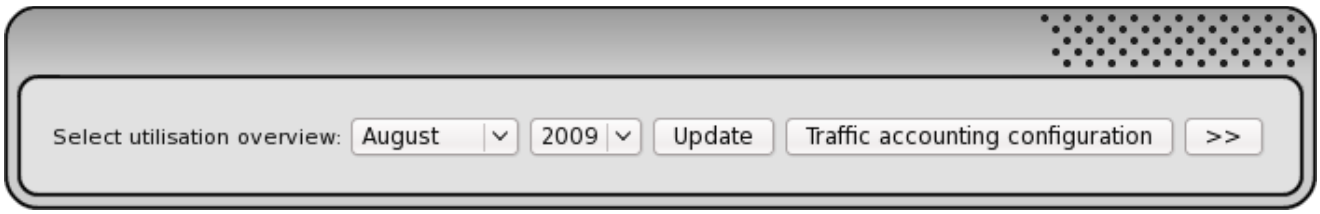
Nota

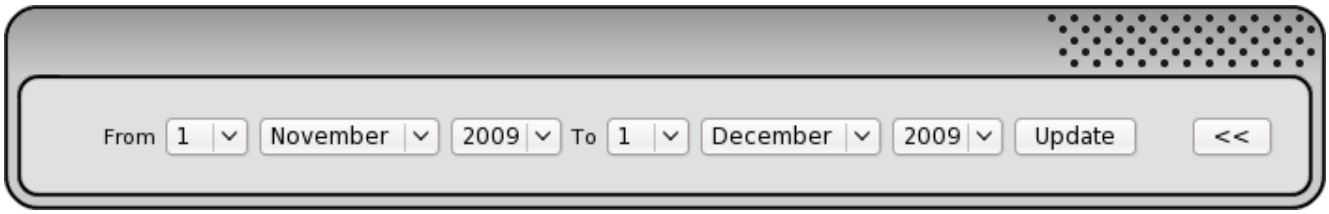
El recuento de tráfico con Nivel de detalle Alto está actualmente desactivado porque no funciona de forma fiable.

2.3.7.1. Selección de Recuento de Tráfico

La primera sección tiene listas desplegables para Mes y Año para seleccionar el período de tiempo.

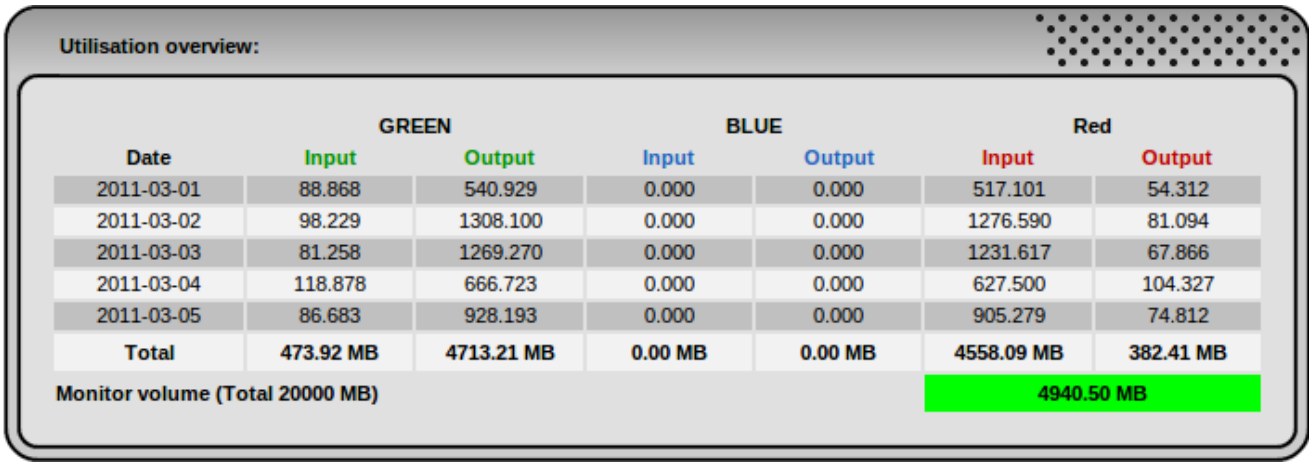
El botón >> abre una segunda caja que le permite seleccionar el rango de tiempo en detalle. Utilice el botón << para volver a la caja de selección estándar.





2.3.7.2. Vista de utilización

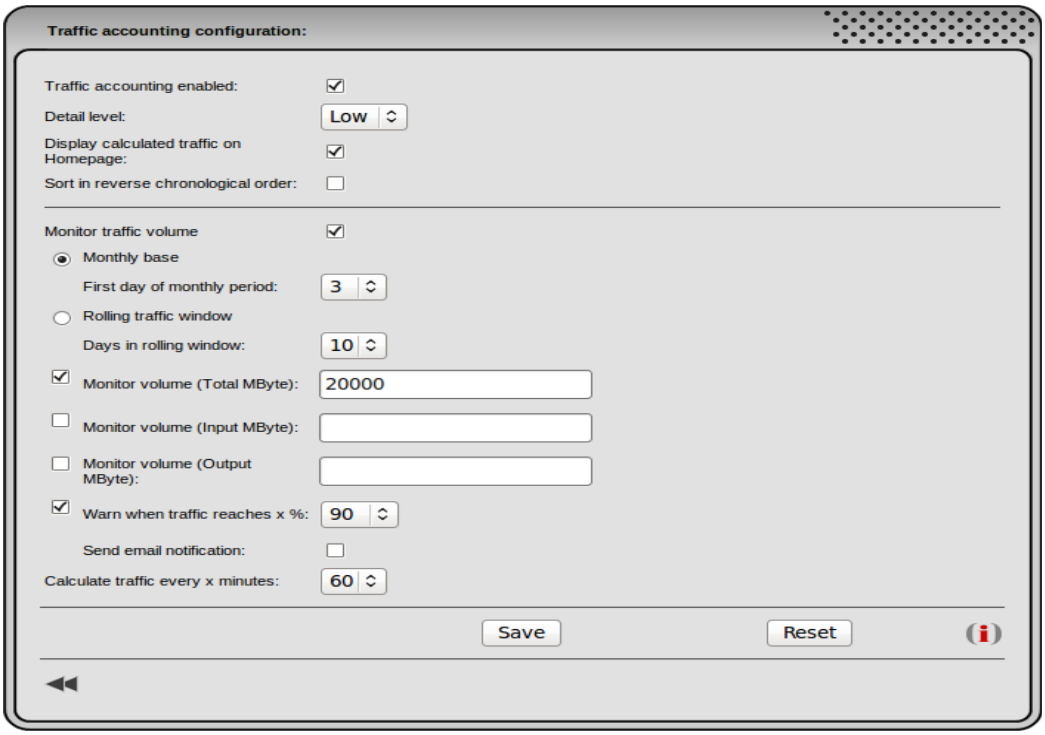
La utilización del tráfico se muestra para cada interfaz configurada. El tráfico de entrada es **hacia** IPCop. El tráfico de salida es **desde** IPCop.



Utilisation overview:

	GREEN		BLUE		Red	
Date	**Input**	**Output**	**Input**	**Output**	**Input**	**Output**
2011-03-01	88.868	540.929	0.000	0.000	517.101	54.312
2011-03-02	98.229	1308.100	0.000	0.000	1276.590	81.094
2011-03-03	81.258	1269.270	0.000	0.000	1231.617	67.866
2011-03-04	118.878	666.723	0.000	0.000	627.500	104.327
2011-03-05	86.683	928.193	0.000	0.000	905.279	74.812
Total	**473.92 MB**	**4713.21 MB**	**0.00 MB**	**0.00 MB**	**4558.09 MB**	**382.41 MB**
Monitor volume (Total 20000 MB)					**4940.50 MB**	

2.3.7.3. Configuración de Recuento de Tráfico



Recuento de Tráfico activado. Marque esta casilla para activar el recuento de tráfico.

Nivel de detalle. Sólo se puede seleccionar Bajo.

Mostrar tráfico calculado en la Página de Inicio. Marque esta casilla para mostrar la información del tráfico en la página de inicio.

Orden cronológico inverso. Marque esta casilla si quiere ver los eventos más recientes al principio de la tabla, en vez de al final.

Monitorizar el volumen de tráfico. Marque esta casilla para activar la monitorización del volumen de tráfico a través de IPCop, que podrá dar un aviso o enviar un correo cuando el tráfico alcance la cantidad indicada.

Ventana mensual o rotatoria. Puede monitorizar el volumen de tráfico en períodos mensuales, o durante un período de tiempo fijo rotatorio, que monitoriza el tráfico durante una ventana de tiempo que va rotando. Puede definir la fecha de inicio del período mensual, o el número de días de la ventana de tiempo.

Monitorizar volumen (...MByte). Puede definir el nivel de monitorización del volumen de tráfico que pasa a través la interfaz Roja de IPCop. Seleccione la casilla apropiada junto a Volumen de entrada, y/o Volumen de salida, y/o Volumen total (que es la combinación del tráfico de entrada y salida) para activar la monitorización. Especifique el volumen en MBytes.

Ahora podrá ver el Monitor de volumen coloreado en la Vista de utilización, con color Verde indicando un volumen por debajo del nivel monitorizado, y Rojo cuando el volumen de tráfico ha excedido el nivel monitorizado.

Avisar cuando el tráfico alcance x %. Marque esta casilla y seleccione un nivel porcentual en el cual se le avisará de que el volumen de tráfico está cercano al nivel del Monitor de volumen.

El color del Monitor de volumen cambia a Naranja en la Vista de utilización, para mostrar que se ha alcanzado el nivel porcentual de advertencia.

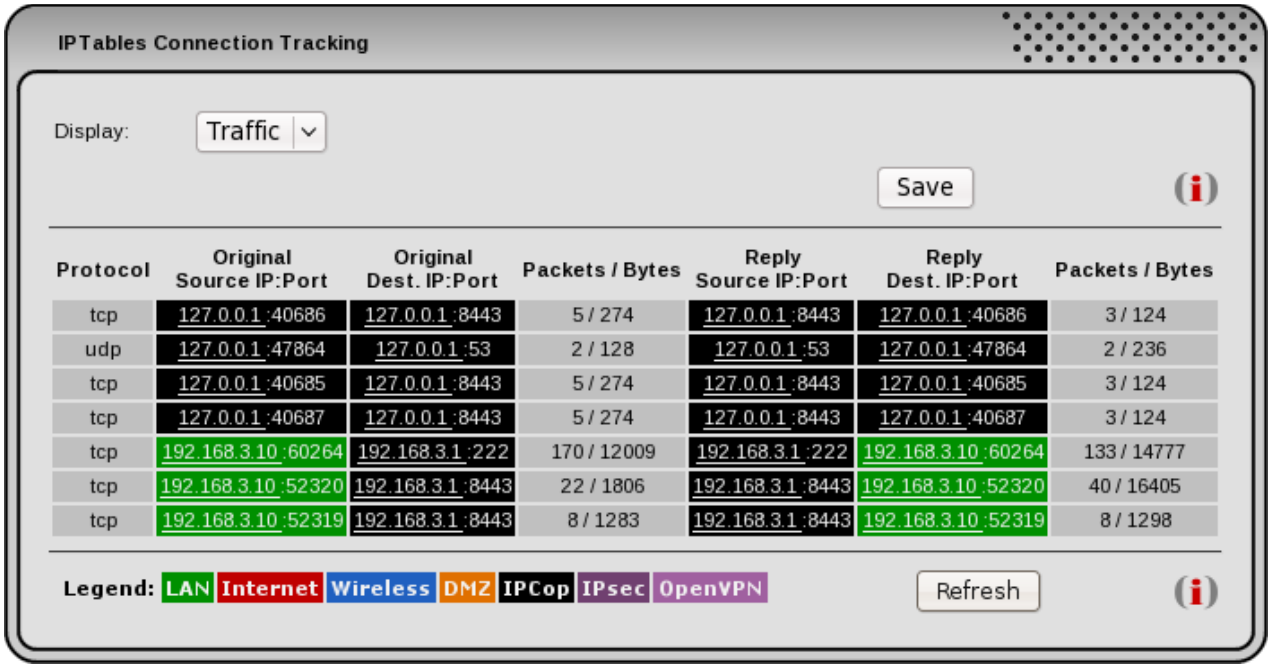
Enviar correo de notificación. Marque esta casilla si quiere que se envíe un “Mensaje de alerta” al destinatario especificado en la página Ajustes de correo cuando el porcentaje de aviso se haya alcanzado.

Calcular tráfico cada x minutos. Puede elegir el período de tiempo entre los cálculos automáticos de volumen de tráfico.

Guardar. Para guardar sus ajustes pulse el botón Guardar.

Reiniciar. El botón Reiniciar revertirá los ajustes a los últimos guardados.

2.3.8. Conexiones

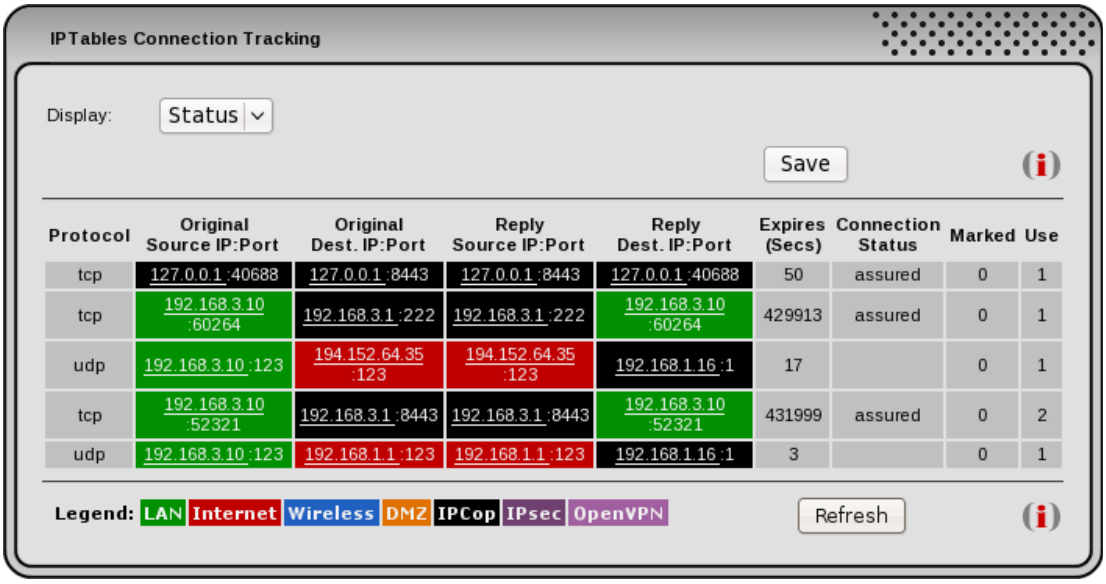


IPCop utiliza la capacidad del cortafuegos Linux Netfilter o IPTables para mantener un cortafuegos 'stateful'. Los cortafuegos 'stateful' siguen la pista de las conexiones a y desde todas las direcciones IP de las redes VERDE, AZUL y NARANJA, basadas tanto en las direcciones IP de origen y destino como en el estado de la propia conexión. Cuando se establece una conexión en la que intervienen máquinas protegidas, sólo a los paquetes con el estado de conexión actual se les permite el paso a través del cortafuegos IPCop.

La ventana Seguimiento de conexiones de IPTables muestra las conexiones de IPTables. Los puntos finales de la conexión están coloreados según su localización en la red. La leyenda de códigos de color se muestra en el pie de página. A continuación se muestra la información de cada conexión individualmente. Se muestran todas las conexiones desde o hacia sus redes.

Elija entre la pantalla de Tráfico y Estado y pulse el botón Guardar para que IPCop recuerde su opción preferida.

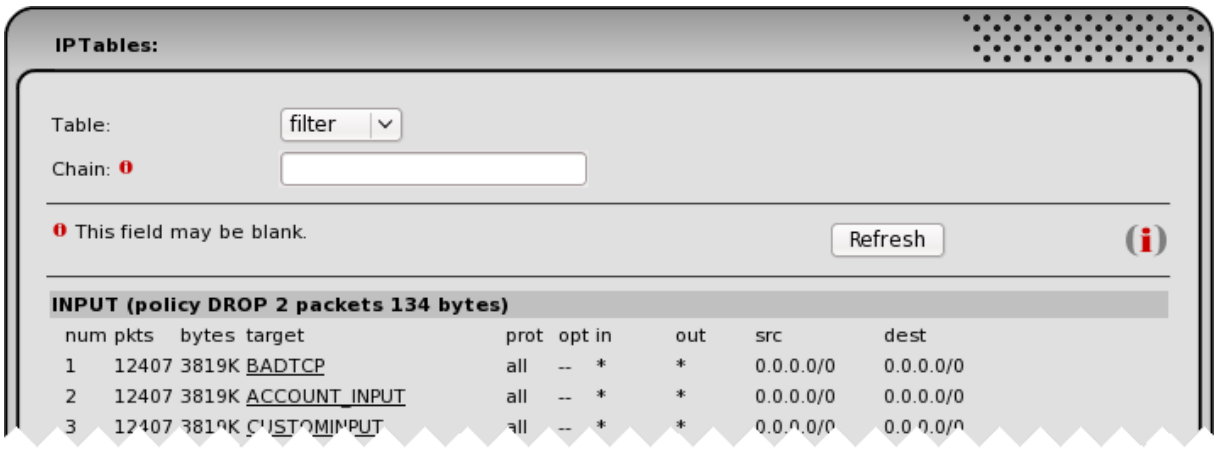
Pulse en una dirección IP para realizar una consulta DNS inversa.



2.3.9. Salida de IPTables

Esta página muestra la salida de IPTables, que puede ser filtrada de varias maneras.

Seleccione un tipo de Tabla del menú desplegable (filter, mangle, nat or raw) y, si lo necesita, teclee el nombre específico (sensible a mayúsculas en el campo Cadena y pulse el botón Refrescar.



2.4. Menú Red

Este grupo de páginas ofrece control sobre algunos de los métodos de conexión de IPCop a Internet. Para acceder a estas páginas, seleccione Red en la barra superior de la pantalla. Aparecerán las siguientes opciones en un menú desplegable:

- Marcado
- Subida
- Módem
- Alias

2.4.1. Marcado

Esta subsección de la ventana de Marcado de la Ventana de Administración (VA) está dividida en cinco secciones editables diferentes y sólo es aplicable si está accediendo a Internet mediante un módem analógico, un dispositivo RDSI o una conexión DSL.

Tenga en cuenta que no puede seleccionar ni modificar un perfil mientras IPCop está en línea o esperando a estarlo en modo“Marcado bajo demanda”. Antes de utilizar esta página, vaya a la VA Inicio y si la línea de estado indica Conectado o Marcado bajo demanda en espera, pulse el botón Desconectar antes de volver a esta ventana. Después de ajustar o selecionar Perfiles, recuerde volver a la VA Inicio y pulsar el botón Conectar si quiere que su IPCop vuelva a estar en línea.

Perfiles. Esta sección proporciona los recursos para enumerar y configurar nuevos Perfiles de Marcado (hasta un total de cinco) o renombrar los Perfiles existentes y modificar sus parámetros.

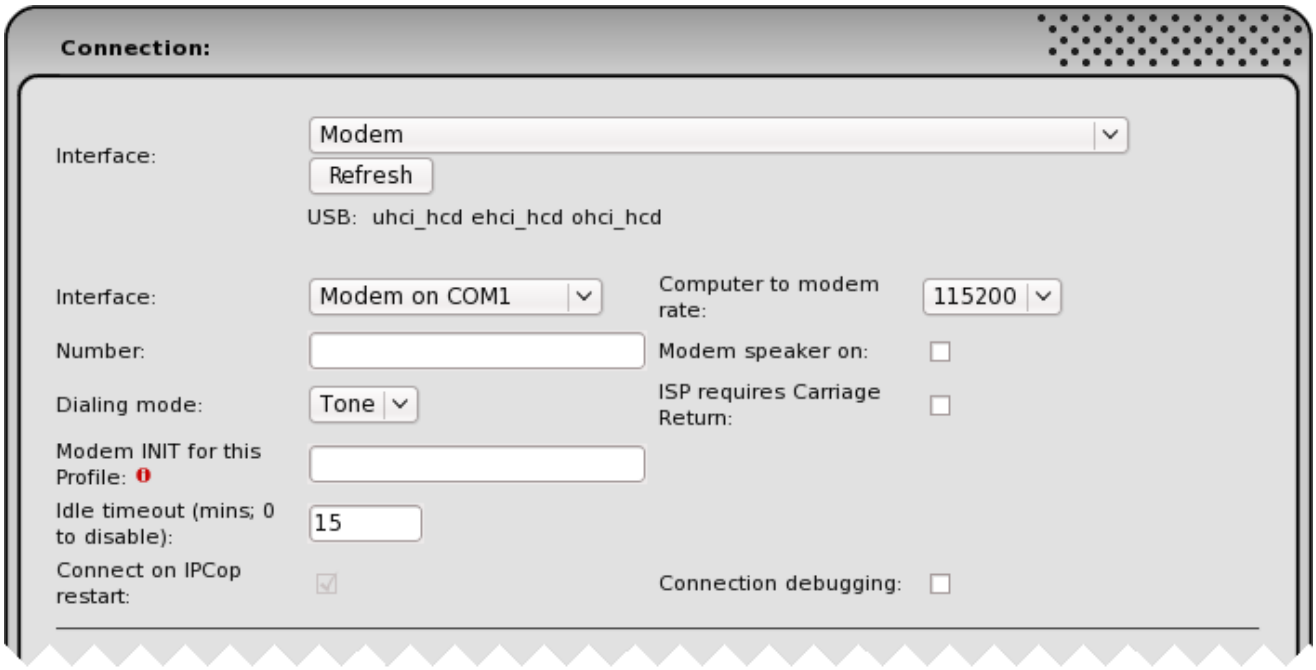
Seleccione un Perfil para crearlo o modificarlo de la lista desplegable. Rellene o cambie los parámetros del perfil (ver abajo) y pulse el botón Guardar. Para seleccionar el Perfil que se usará en futuras conexiones, utilice la lista desplegable para elegirlo y pulse el botón Seleccionar en la parte inferior

de la pantalla. Utilice el botón Restaurar mientras esté editando un Perfil para recuperar los ajustes previos.

Figura 2.15. Perfiles de Conexión

Conexión. Seleccione el tipo de Interfaz adecuada a su dispositivo de conexión a Internet de la lista desplegable y pulse el botón Refrescar para rellenar la sección Conexión con el contenido relativo a su dispositivo.

Figura 2.16. Interfaz de conexión



1. Interfaz. Ésta será o bien un puerto de comunicaciones (COM1-COM5, ttyUSB0-4, noz0-1, ttyHS0-3, o usb/ttyACM0-3), empleado mayoritariamente por módems y tarjetas RDSI, o bien PPPoE, empleado principalmente por conexiones DSL.

2. Seleccione la tasa ordenador a módem adecuado. Esto decidirá cómo de rápido se pasan los datos hacia y desde su dispositivo de conexión. Con ordenadores muy antiguos o módems, puede que sea necesario emplear uno de los valores más bajos de tasa de transferencia para establecer una comunicación fiable entre ordenador y módem.

3. Introduzca el número correcto para marcar según su conexión a Internet. Si se está conectando mediante una interfaz PPPoE, probablemente deberá dejar esto en blanco.

4. Altavoz del módem activado. Marque esta casilla si quiere activar el altavoz del módem. Con el altavoz activo puede oír cómo tiene lugar la conexión, lo cual puede ayudarle a diagnosticar un problema. Esta opción sólo es útil si se está conectando mediante un módem analógico.

5. Seleccione su Modo de marcado. Utilice Marcado por tonos a menos que su conexión telefónica sólo reconozca el Marcado por pulsos. El Marcado por pulsos es mucho más lento que el Marcado por tonos.

6. ISP Requiere retorno de carro. Algunos ISPs requieren que el módem envíe un retorno de carro para indicar que ha terminado de enviar datos. Si su ISP requiere esto, marque esta casilla. Por defecto está desmarcada.

7. Secuencia INIT para este Perfil - opcional. Este campo está disponible para el caso de que necesite proporcionar una cadena INIT a su módem para *este Perfil concreto*, además de la cadena INIT normal del módem.

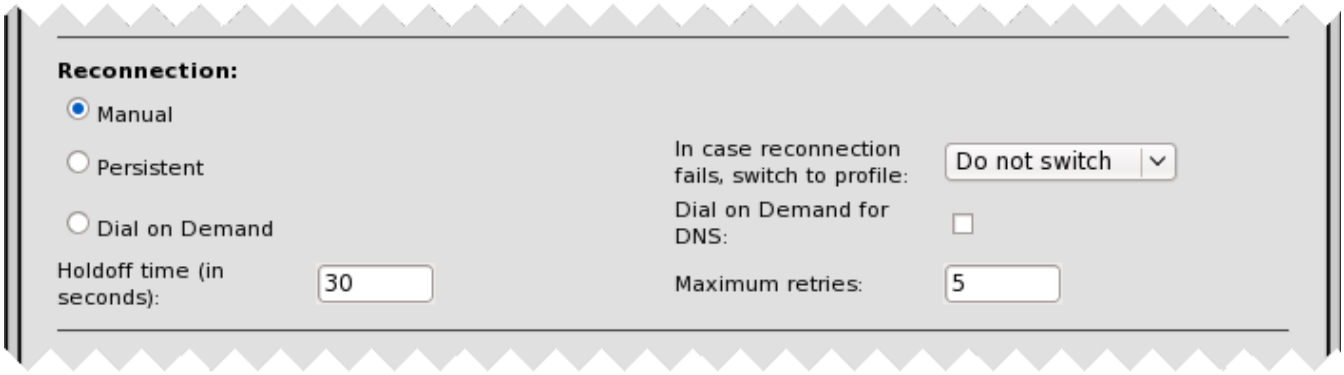
8. Introduzca su Tiempo de inactividad. Esto decidirá cómo maneja IPCop su conexión a Internet cuando no se está enviando o recibiendo nada a través de la conexión a Internet. El número introducido aquí indica a IPCOP cuánto debe esperar tras cualquier actividad de Internet antes de desconectar el enlace del módem. Si pone este parámetro a 0, IPCop no realizará ninguna desconexión una vez que se haya conectado.

9. Conectar al reinicio de IPCop hará que IPCop se conecte tras el arranque si no se ha seleccionado Marcado bajo demanda.

   Probablemente quiera activar esta opción incluso si está empleando Marcado bajo demanda. La combinación de ajustes hará que IPCop se ponga en modo de espera para Marcado bajo demanda cada vez que IPCop se enciende o reinicia.

10. Diagnóstico de conexión. Marque esta casilla para escribir información adicional en la sección ROJA de los Registros del sistema. Esto puede resultar muy útil para diagnosticar situaciones de “fallo al conectar”.

Figura 2.17. Conectar/Reconectar



Reconectar. Puede reconectar de uno de estos tres métodos: Manual, Persistente y Marcado bajo demanda.

1. Con el método Manual tendrá que pulsar el botón Conectar de la página de Inicio.

2. La opción de conexión Persistente se utiliza para decirle a IPCop que mantenga la conexión a Internet en todo momento, incluso en ausencia de actividad de Internet.

   En este modo, se intentará reconectar a Internet cada vez que el enlace falle por cualquier motivo, como una desconexión por tiempo desde el lado del enlace del módem del ISP.

   Utilice este modo con cuidado. Si tiene facturación por conexión, probablemente no quiera emplear este modo. Por otra parte, si tiene tarifa plana ilimitada con su ISP, puede querer activar esta opción para mantener el enlace conectado siempre que sea posible.

Observe que en modo Persistente, IPCop dejará de reconectarse tras superar el número de conexiones fallidas sucesivas indicado en Intentos máximos. En este caso, deberá emplear el botón Conectar de la página de Inicio.

3. Marcado bajo Demanda está disponible seleccionando la opción correspondiente. Tenga en cuenta que tras activar el Marcado bajo Demanda, aún deberá pulsar el botón Connect en la página de inicio para que IPCop empiece a conectarse cuando detecte actividad de Internet. La opción Marcado bajo Demanda no está disponible para conexiones PPPoE.

4. El menú desplegable En caso de fallo de conexión, cambiar al perfil permite seleccionar un perfil alternativo por si su conexión principal falla.

5. La opción Marcado bajo Demanda para DNS determina si IPCop se conectará automáticamente cuando detecte peticiones DNS. Generalmente, este es el comportamiento deseado.

6. El Tiempo de espera es el período, en segundos, que IPCop deberá esperar entre reintentos. Por defecto es treinta segundos.

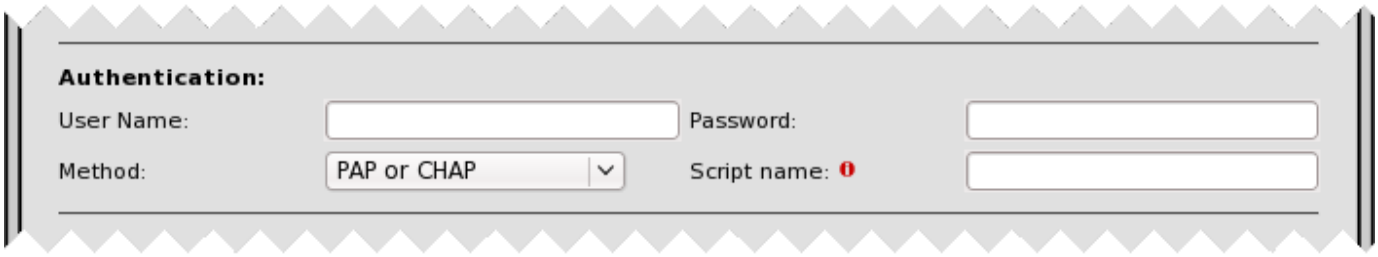
7. Introduzca el número deseado de Reintentos máximos. Esto decidirá con qué frecuencia IPCop se intentará conectar tras una conexión fallida.

Ajustes de ADSL. Tanto si está activado PPPoE como USB ADSL, habrá disponibles opciones adicionales.

En esta sección puede seleccionar diferentes protocolos, métodos de encapsulación, o añadir parámetros opcionales, como un nombre del servicio, o un nombre de concentrador, que algunos ISPs requieren. Si su ISP no los requiere, o no le ha proporcionado ninguno, puede dejar estos dos campos en blanco.

Su ISP le dará dos parámetros, VPI y VCI, que deberá introducir si está utilizando una conexión USB ADSL.

Figura 2.18. Autenticación

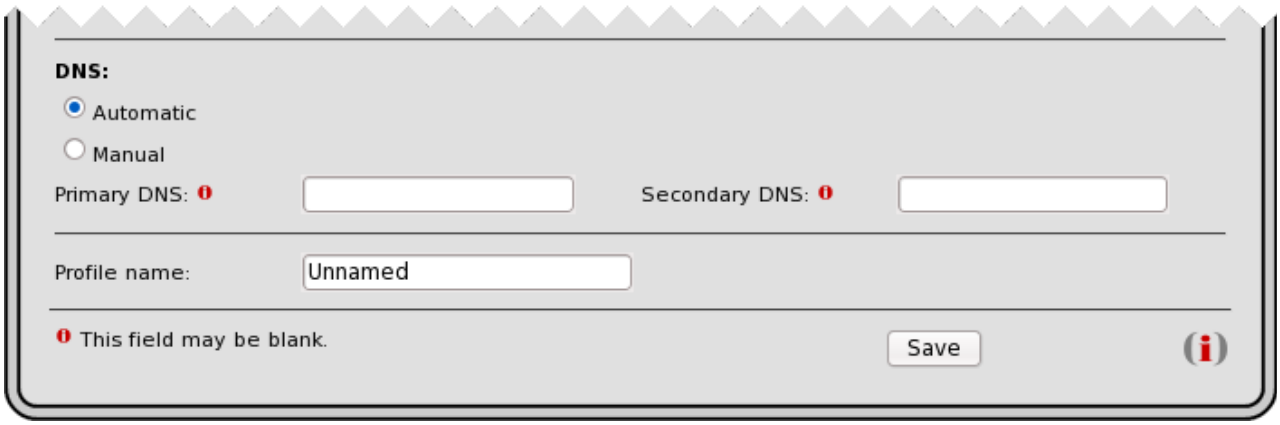


Autenticación. El Nombre de Usuario y la Contraseña son el nombre de usuario y la contraseña que su ISP debería haberle proporcionado al contratar el servicio.

Hay varias maneras mediante las que los ISPs utilizan este nombre de usuario y contraseña para autenticarse en sus sistemas. Los metodos más comunes son PAP o CHAP. Seleccione el adecuado si su ISP emplea uno de ellos.

En el caso poco probable de que su ISP utilice un script de texto para autenticarse, necesitará acceder a IPCop y crear un archivo en el directorio `/etc/ppp/`. El nombre de este archivo (sin el prefijo `/etc/ppp/`) deberá ser indicado en el campo Nombre de Script. El archivo debe contener pares 'expect send', separados por un tabulador. Examine el archivo `/etc/ppp/demonloginscript` para ver un ejemplo de lo debería haber en este archivo. *`USERNAME`* se sustituirá por el nombre de usuario y *`PASSWORD`* por la contraseña.

Figura 2.19. DNS



DNS. Seleccione Automático si su ISP soporta la configuración automática de servidores DNS, como suele ser habitual. Alternativamente, seleccione Manual y ponga las direcciones IP en los campos DNS Primario y DNS Secundario. Estas direcciones IP serán indicadas por su ISP, cuando sean necesarias.

Nombre de Perfil. Para nombrar, o renombrar, un perfil, introduzca el nombre en este campo.

Guardar. Para guardar su configuración, pulse el botón Guardar.

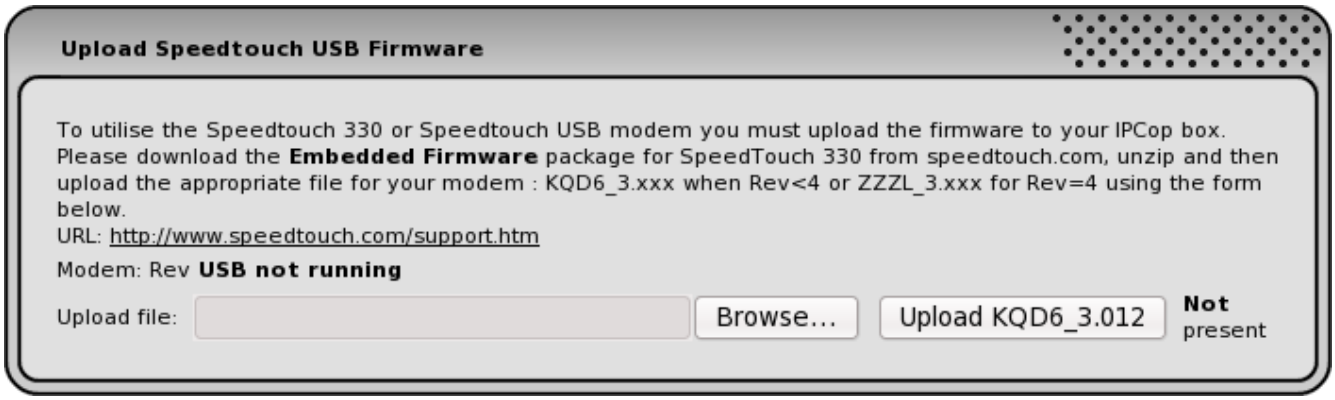
2.4.2. Subidas

Utilice esta página para descargar los archivos necesarios para soportar diferentes módems a su ordenador y luego subirlos a su IPCop.

2.4.2.1. Subir Firmware Speedtouch USB

Utilice esta sección para subir el archivo del firmware a IPCop - Speedtouch USB ADSL no funcionará hasta que esto se haya hecho.

Figura 2.20. Sección típica de subida de firmware



Necesitará un archivo para los módems Speedtouch Revisión 4, y otro distinto para modelos anteriores. Utilice el archivo `KQD6_3.012` para las Revisiones 1 y 2, y el archivo `ZZZL_3.012` para los módems Revisión 4.

Si conecta su módem Speedtouch al IPCop, IPCop detectará la versión y mostrará el archivo correcto para subir.

Localice el archivo zip del firmware Speedtouch en Internet, descárguelo y extraiga los archivos en su ordenador. A continuación, seleccione el archivo adecuado en su ordenador y use el botón Subir para transferirlo al IPCop.

En este momento, una vez que haya subido el archivo, necesitará abrir una consola como 'root' en IPCop y ejecutar los siguientes comandos para extraer los archivos del firmware y moverlos al lugar correcto. (N.B. el ejemplo siguiente es para un módem Revisión 1 ó 2, el archivo para un módem Revisión 4 se llama `firmware.v4_b.bin`).

```
$ cd /var/ipcop/alcatelusb/
$ /usr/sbin/firmware-extractor firmware.v0123.bin
```

Esto creará dos archivos en el directorio `/var/ipcop/alcatelusb/`, `speedtch-1.bin` y `speedtch-2.bin`. Estos dos archivos necesitan ser movidos al directorio `/lib/firmware/` con este comando:

```
$ mv speedtch-1.bin speedtch-2.bin /lib/firmware/
```

Una vez que haya hecho esto, podrá usar su módem Speedtouch USB ADSL. Puede que necesite reiniciar IPCop.

Probablemente, también quiera añadir `/lib/firmware/speedtch-1.bin` y `/lib/firmware/speedtch-2.bin` a `/var/ipcop/backup/include.user` para que los archivos sean incluidos automáticamente en una Restauración de Sistema.

2.4.2.2. Subir archivo ECI ADSL Synch.bin

Utilice esta sección para subir el archivo `synch.bin` al IPCop - ECI ADSL no funcionará hasta que esto se haya hecho. Utilice el enlace especificado para ir a la página web y descargar el archivo a su ordenador. Luego elija el archivo de su ordenador, y pulse el botón Subir para transferirlo al IPCop.

Una vez que se haya subido con éxito, podrá usar ECI ADSL.

2.4.2.3. Subir driver Fritz!DSL

Utilice esta sección para subir el archivo `ipcop-<version>-install-avmdrv.i486.tgz` al IPCop - Fritz!DSL no funcionará hasta que esto se haya hecho. Utilice el enlace especificado para ir a la página web y descargar el archivo a su ordenador. Luego elija el archivo de su ordenador, y pulse el botón Subir para transferirlo al IPCop.

Una vez que se haya subido con éxito, podrá usar Fritz!DSL.

Nota

El driver Fritz!DSL está disponible únicamente para arquitectura x86.

2.4.3. Módem

Esta sección sólo es aplicable si está intentando conectarse a Internet con un módem analógico estándar.

2.4.3.1. Configuración del módem

Los ajustes por defecto que aparecen en esta página son apropiados para la mayoría de módems analógicos. De todas formas, si experimenta problemas al conectarse, compare estos ajustes con los

sugeridos en el manual del módem para uso con su módem en particular. La mayoría de estos ajustes se pueden dejar en blanco.

Figura 2.21. Ajustes del módem

Init (opcional). La cadena de inicialización empleada por la mayoría de módems compatibles Hayes está puesta en este campo. Si por alguna razón, su módem requiere un ajuste diferente cámbielo.

Dos módems, cadenas Init diferentes

Si tiene un segundo módem en su IPCop, como conexión de reserva en otro perfil, por ejemplo, y cada módem requiere una cadena de inicialización diferente, utilice el campo “Módem INIT para este Perfil” previsto para este caso en la página Marcado.

Colgado (opcional). La cadena HANG UP empleada por la mayoría de módems compatibles Hayes ya está puesta en este campo. Cámbiela en caso necesario.

Altavoz activado (opcional). La cadena SPEAKER ON estándar empleada por la mayoría de módems compatibles Hayes ya está puesta en este campo. Cámbiela en caso necesario.

Altavoz desactivado (opcional). La cadena SPEAKER OFF estándar empleada por la mayoría de módems compatibles Hayes ya está puesta en este campo. Cámbiela en caso necesario.

Marcado por tonos (opcional). La cadena TONE DIAL estándar empleada por la mayoría de módems compatibles Hayes ya está puesta en este campo. Si su módem y línea telefónica soportan el marcado por tonos y experimenta problemas al conectarse, asegúrese de que esta cadena es la apropiada para su módem.

Marcado por pulsos (opcional). La cadena PULSE DIAL estándar empleada por la mayoría de módems compatibles Hayes ya está puesta en este campo. No debería ser necesario cambiarla, pero si su servicio telefónico no soporta el marcado por tonos, puede que necesite asegurarse de que ésta es la cadena correcta para su módem.

Tiempo de espera de Conexión. El único campo en esta sección que no puede quedar en blanco es el Tiempo de espera de Conexión. Esto le dice a IPCop cuánto tiempo permite al módem intentar conectar. Tras pasar este número de segundos sin una respuesta apropiada del otro extremo, IPCop dejará el intento y pasará al siguiente intento de conexión. El valor por defecto debería funcionar bien, pero si nota que la conexión se cae durante la secuencia de negociación (encienda el altavoz del módem y escúche los intentos de conexión) podría necesitar aumentar este parámetro ligeramente, hasta que se conecte con éxito.

Restaurar valores por defecto. Para restaurar los valores por defecto, pulse el botón Restaurar valores por defecto, y luego el botón Guardar.

Guardar. Para guardar su configuración pulse el botón Guardar.

2.4.4. Página administrativa Alias Externos

Nota

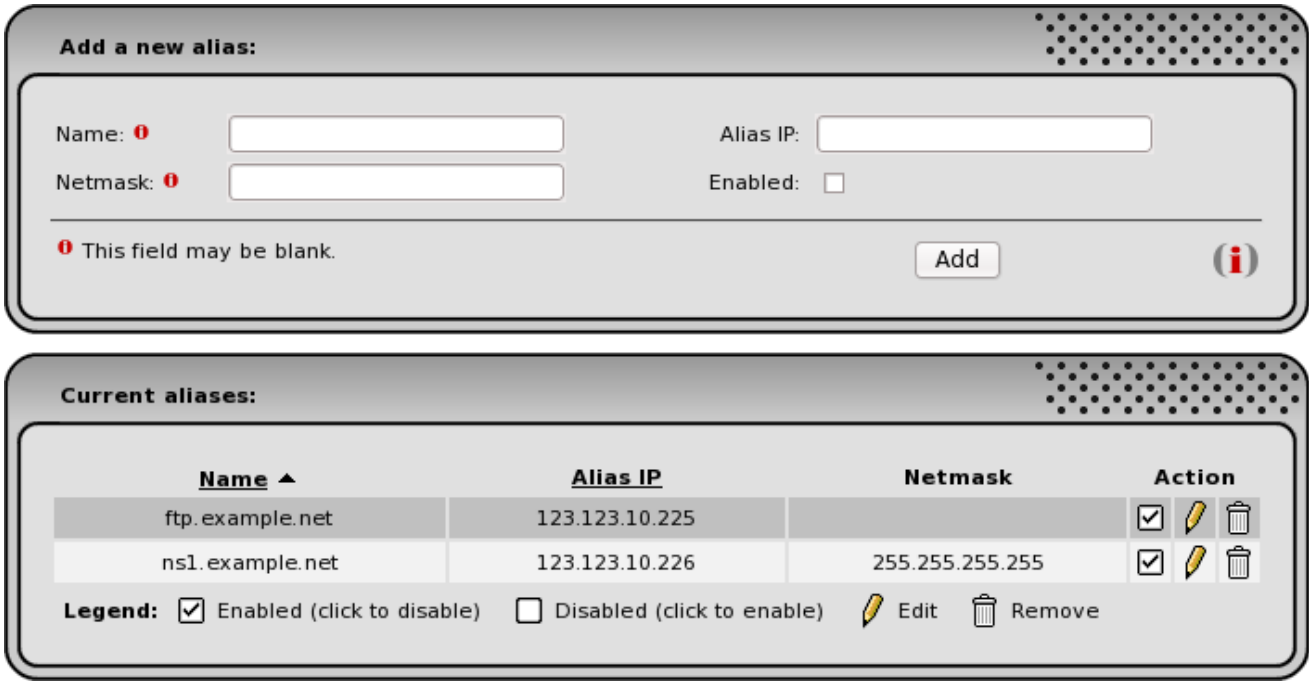
Los alias sólo se activarán si su interfaz ROJA es ESTÁTICA.

Puede ser que su ISP le asigne un rango de direcciones IP para su red. **Sólo** necesitará esas direcciones IP adicionales en caso de que quiera ofrecer **múltiples** servicios como servidor de Internet y desee que esos servicios sean alcanzables con diferentes direcciones o nombres.

2.4.4.1. Añadir un nuevo alias

Añade o edita un alias en la primera sección.

Figura 2.22. Secciones Alias



Nombre (opcional). Dé un nombre al alias si lo desea.

IP de Alias. Introduzca una dirección IP.

Máscara de red (opcional). Especifique una máscara de red si es necesario.

Activado. Marque esta casilla para activar la entrada.

Añadir. Una vez que ha introducido toda la información, pulse el botón Añadir Esto moverá la entrada a la siguiente sección, y se listará como un alias.

2.4.4.2. Alias actuales

Esta sección lista los alias que usted ha añadido.

Puede reordenar la lista pinchando en cualquiera de las cabeceras de columna que están subrayadas. Si vuelve a pinchar, invertirá el orden del listado.

Para activar o desactivar una entrada, pinche en la casilla de la columna Acción del alias que desee activar o desactivar. El icono cambia a una casilla vacía cuando la entrada está desactivada. Pinche en la casilla para activarla de nuevo.

Para editar una entrada, pinche en su icono de *lápiz amarillo*. Los datos de la entrada se mostrarán en el formulario superior. Realice los cambios y pulse el botón Actualizar en el formulario.

Para borrar una entrada, pinche en el icono de su *papelera*.

2.5. Menú Servicios

Además de realizar su función principal como cortafuegos de Internet, IPCop puede proveer varios servicios de utilidad en una pequeña red.

Éstos son:

- Proxy (Servidor proxy web)
- Filtro URL (Bloquea el acceso a dominios, URLs o archivos no deseados)
- Servidor DHCP
- Gestión de DNS dinámico
- Edición de Hosts (Servidor DNS local)
- Servidor de hora
- Priorización de tráfico

En una red más grande, es probable que algunos de estos servicios estén siendo proporcionados por servidores dedicados y deberían desactivarse aquí.

2.5.1. Página administrativa del Proxy web

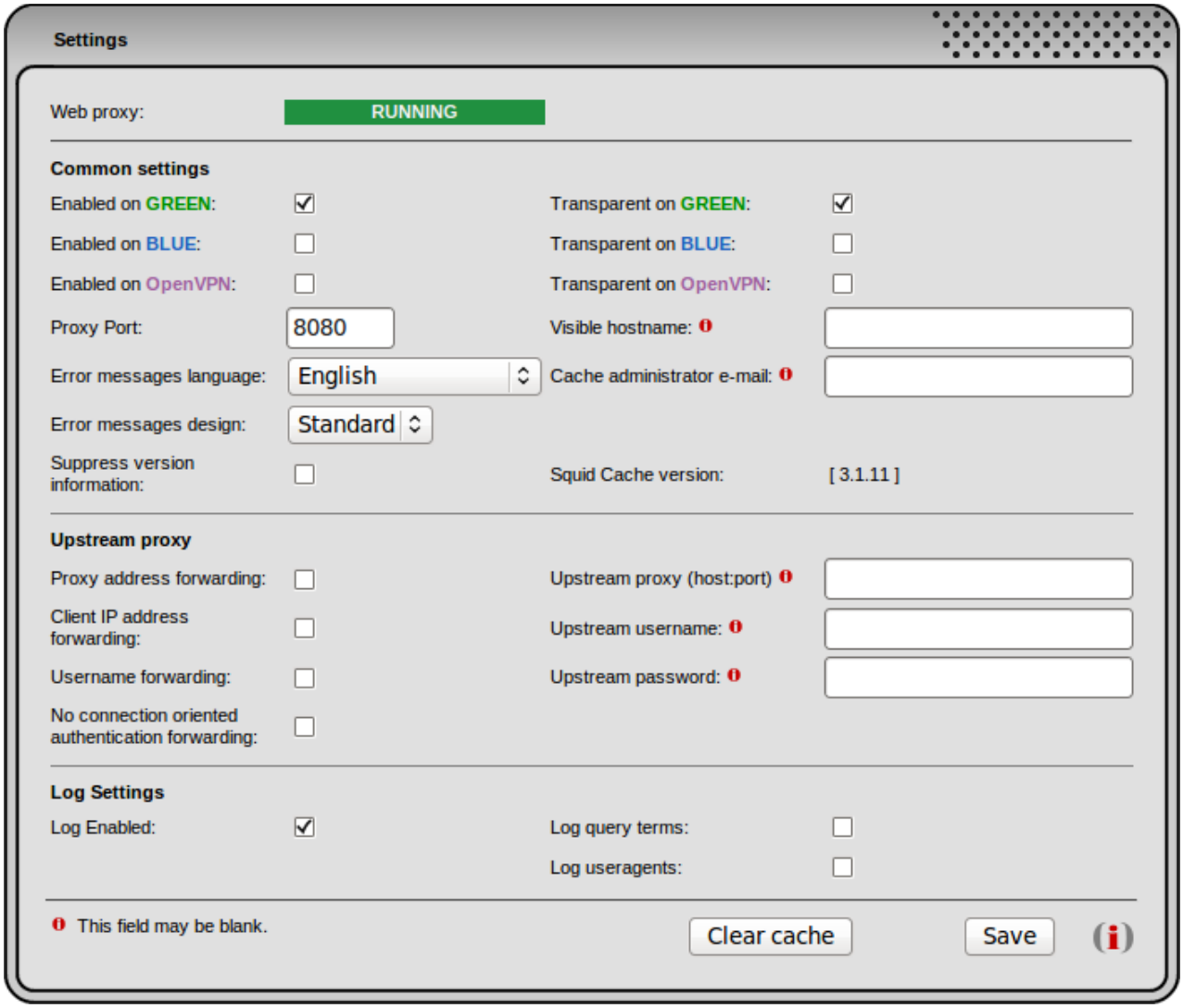
Un servidor proxy es un programa que realiza las peticiones de páginas web en lugar de todas las máquinas de su intranet. El servidor proxy guardará en caché las páginas que recibe de la web, de manera que si tres máquinas piden la misma página, sólo se necesitará una transferencia desde Internet. Si su organización tiene varias páginas de uso habitual, esto puede ahorrar accesos a Internet.

Normalmente, deberá configurar los navegadores utilizados en su red para que usen el servidor proxy para acceder a Internet. Debe poner el nombre/dirección de la máquina IPCop como proxy y el puerto que introdujo en la casilla Puerto del Proxy, por defecto el 8080. Esta configuración permite a los navegadores evitar el proxy si lo desean. También es posible correr el proxy en modo “transparente”. En este caso, los navegadores no necesitan ninguna configuración especial y el cortafuegos redirecciona automáticamente todo el tráfico sobre el puerto 80, el puerto estándar HTTP, al servidor proxy.

2.5.1.1. Proxy web

La primera línea en la casilla Ajustes indica si el proxy está parado o corriendo.

Figura 2.23. Proxy web - Secciones de Ajustes comunes, Proxy siguiente & Ajustes del registro



2.5.1.2. Ajustes comunes

Puede elegir si quiere mandar las peticiones al proxy desde su red Verde (privada) y/o su red Azul (inalámbrica, si existe). Simplemente marque las casillas correspondientes.

Activado en... Marque la casilla apropiada para activar el servidor proxy para que escuche peticiones en la interfaz seleccionada (Verde o Azul). Si el servidor proxy está desactivado, todas las peticiones de los clientes se reenviarán directamente a la dirección de destino.

Transparente en... Si el "modo transparente" está activado, todas las peticiones con destino al puerto 80 serán reenviadas al servidor proxy sin necesidad de configurar de forma especial sus clientes.

Puerto del proxy. Este es el puerto en el que el servidor proxy escuchará las peticiones de los clientes. Por defecto es el 8080. En modo transparente, todas las peticiones al puerto 80 serán automáticamente redireccionadas a este puerto.

Nombre de host visible - opcional. Si quiere mostrar un nombre de host diferente en los mensajes de error del servidor proxy o para los servidores proxy siguientes, especifíquelo aquí. Si lo deja en blanco, se usará en nombre de host real de su IPCop.

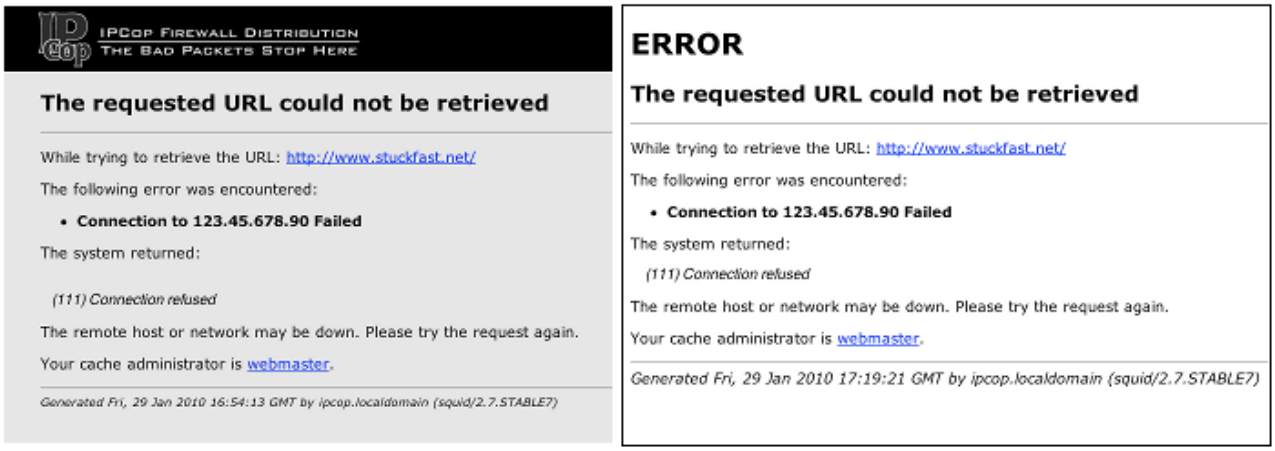
Correo del Administrador de la caché - opcional. Puede especificar una dirección de correo que aparecerá en los mensajes de error del servidor proxy a los clientes. Si lo deja en blanco, se usará "webmaster" en su lugar.

Idioma de los mensajes de error. Puede elegir el idioma en el que se mostrará cualquier error del servidor proxy a los clientes.

Diseño de los mensajes de error. Puede elegir el estilo en el que se mostrarán los errores del servidor proxy a los clientes. Puede elegir entre "IPCop" y "Estándar".

El diseño IPCop incluye un bonito banner gráfico, mientras que el diseño estándar es el habitual que incluye Squid.

Figura 2.24. Diseños de mensaje de error del proxy. IPCop a la izquierda, Estándar a la derecha.



Nota

Si define un If you define a Nombre de host visible (ver más arriba), se usará *siempre* el diseño Estándar.

Suprimir información de la versión. Marque esta casilla para evitar mostrar la versión de la caché de Squid en los mensajes de error de Squid a los clientes.

Versión de caché de Squid. Esto indica la versión de caché de Squid instalada.

2.5.1.3. Proxy siguiente

Estos ajustes pueden ser necesarios en entornos con proxys encadenados.

Si su proveedor le solicita que utilice su caché para el acceso web, deberá especificar el nombre de host y el puerto en la casilla de texto Proxy siguiente. Si el proxy de su proveedor requiere un nombre de usuario y contraseña, introdúzcalos en los campos Nombre de usuario del siguiente Proxy y Contraseña del siguiente Proxy.

Reenvío de la dirección del proxy. Esto activa el campo de la cabecera HTTP VIA. Si está activado, se añadirá esta información a la cabecera HTTP:

```
1.0 ipcop.localdomain:8080 (Squid/2.7.STABLE7)
```

Nota

¡Si el último proxy de la cadena no elimina este campo, se reenviará al host de destino!

Este campo se suprimirá por defecto.

Reenvío de la dirección IP del cliente. Esto activa el campo de la cabecera HTTP X-FORWARDED-FOR. Si está activado, se añadirá la dirección interna del cliente a la cabecera HTTP, p.e.: `192.168.1.30`

Esto puede ser útil para ACLs (listas de control de acceso) basadas en el origen o para acceder a servidores proxy remotos.

Nota

¡Si el último proxy de la cadena no elimina este campo, se reenviará al host de destino!

En vez de reenviar "desconocido", este campo se eliminará completamente por defecto.

Reenviar nombre de usuario. Si hay cualquier tipo de autenticación activada, esto activa el reenvío del nombre de usuario.

Esto puede ser útil para ACLs (listas de control de acceso) basadas en el origen o para acceder a servidores proxy remotos.

Nota

Esto es sólo para uso de ACL o registro, y no funciona si el siguiente proxy requiere un login real.

Este reenvío está limitado al nombre de usuario. La contraseña no se reenviará.

Reenvío de autenticación no orientada a conexión. Esto desactiva el reenvío de la conexión orientada a conexión de Microsoft (NTLM y Kerberos).

2.5.1.4. Ajustes del registro

Registro activado. Si elige activar el proxy, puede también registrar los accesos web marcando la casilla Registro activado. Esto activa también el sistema de registro del servidor proxy, que puede ser útil para la resolución de problemas.

Los accesos realizados a través del proxy pueden verse visitando la página Registros del proxy.

El registro también debe ser activado para que funcionen los Gráficos del Proxy.

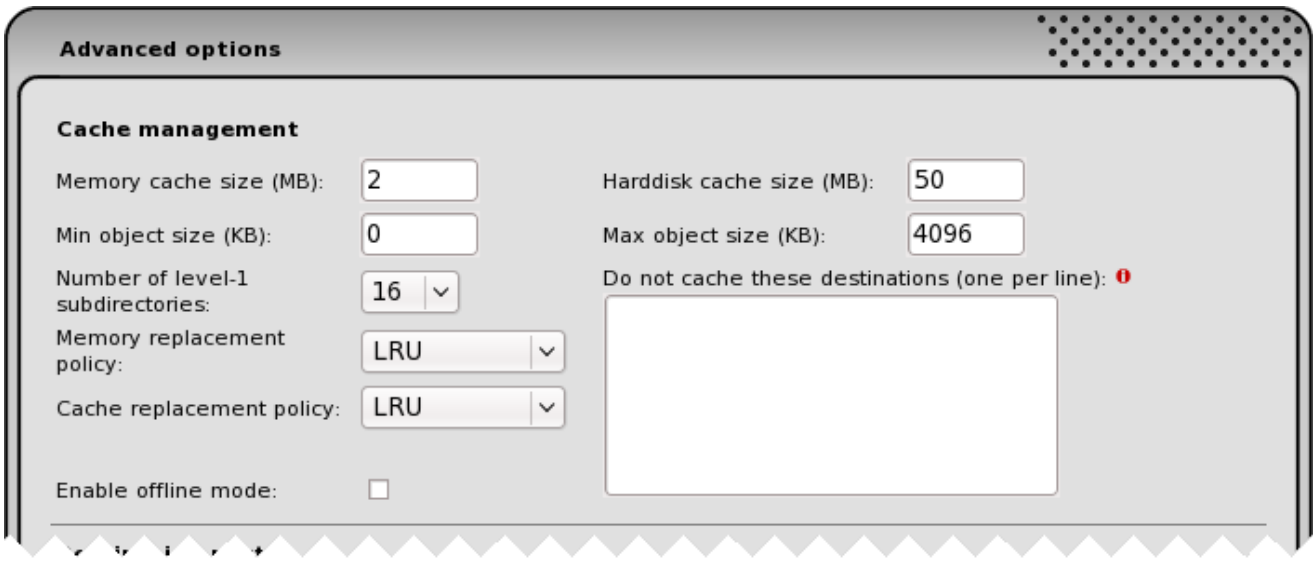
Registrar términos de búsqueda. La parte de la URL que contiene búsquedas dinámicas se eliminará por defecto antes de su registro. Activando la opción "Registrar términos de búsqueda" se desactivará esto y se registrará la URL completa.

Registrar useragents. Activar "Registrar useragents" escribirá la cadena useragent en el archivo de registro `/var/log/squid/user_agent.log` Esta opción del archivo de registro sólo debería activarse para búsqueda de fallos y los resultados no se muestran con el visor de registros basado en GUI.

2.5.1.5. Gestión de caché

Puede elegir cuánto espacio de disco debería ser utilizado para cachear páginas web en la sección Gestión de caché. También puede ajustar el tamaño del objeto más pequeño a cachear, normalmente 0, y el más grande, 4096 KB.

Por razones de privacidad, el proxy no cacheará páginas recibidas mediante HTTPS, u otras páginas en las que se envía un nombre de usuario y una contraseña mediante la URL.



Aviso

Cachear puede ocupar mucho espacio en su disco duro. Si emplea una caché grande, el tamaño mínimo de disco indicado en la documentación de IPCop *no* sera suficientemente grande.

Cuando mayor sea la caché que defina, más memoria necesitará el servidor proxy para gestionar la caché. Si está corriendo IPCop en una máquina con poca memoria no elija una caché grande.

Tamaño de memoria para caché. Esta es la cantidad de memoria física que se usará para los objetos no cacheados y en tránsito. Este valor no debería ser mayor del 50% de la memoria RAM instalada. El mínimo para este valor es de 1 MB, y por defecto es de 2 MB.

Este parámetro no especifica el tamaño máximmo de un proceso. Sólo pone un límite a cuánta RAM adicional usará el proxy como caché de objetos.

Tamaño de caché en disco. Esta es la cantidad de espacio en disco, en MB, que se usará para objetos cacheados. Por defecto es 50 MB. Cambie esto para ajustarse a su configuración. No ponga el tamaño de su disco aquí. En su lugar, si quiere que **squid** use todo el disco, reste un 20% y utilice ese valor.

¿Cómo hago que IPCop sea sólo proxy, sin cachear nada?

Ponga el Tamaño de memoria para caché y el Tamaño de caché en disco **ambos** a 0, para desactivar la caché por completo.

Tamaño mínimo de objeto. Los objetos menores que este tamaño no se guardarán en disco. El valor se especifica en kilobytes, y por defecto es de 0 KB, lo que significa que no hay mínimo.

Tamaño máximo de objeto. Los objetos mayores que este tamaño no se guardarán en disco. El valor se especifica en kilobytes, y por defecto es de 4 MB. Si quiere aumentar la velocidad, más que ahorrar ancho de banda, debe dejar esto bajo.

Número de subdirectorios de nivel 1. El valor por defecto para la caché en disco duro de subdirectorios de nivel 1 es 16.

Cada directorio de nivel 1 contiene 256 subdirectorios, por lo que un valor de 256 directorios de nivel 1 usará un total de 65536 directorios para la caché en disco duro. Esto ralentizará notablemente el proceso de inicio del servicio de proxy pero puede acelerar el cacheo bajo ciertas condiciones.

Nota

El valor recomendado para directorios de nivel 1 es 16. Debería aumentar este valor sólo cuando sea necesario.

Política de reemplazo de memoria. El parámetro política de reemplazo de memoria determina qué objetos son eliminados de la memoria cuando se necesita espacio de memoria. La política por defecto en IPCop es LRU.

Políticas de reemplazo posibles son:

LRU

> La política original de Squid basada en lista de Último Usado Recientemente (Last Recently Used). La política LRU mantiene los objetos referenciados recientemente. Por ejemplo, reemplaza el objeto que no ha sido accedido por más tiempo.

heap GDSF

> La política heap Greedy-Dual Size Frequency optimiza el ratio de aciertos por objeto manteniendo los objetos menores más populares en caché, por lo que tiene más posibilidades de tener un acierto. Aun así, consigue un menor ratio de acierto en bytes que LFUDA, ya que evita objetos mayores (posiblemente populares).

heap LFUDA

> Menor Frecuencia de Uso con Edad Dinámica (Least Frequently Used with Dynamic Aging). Esta política mantiene objetos populares en caché independientemente de su tamaño, por lo que optimiza el ratio de aciertos en bytes a costa de del ratio de aciertos por objeto, ya que un objeto grande y popular evitará que muchos objetos menores y un poco menos populares sean cacheados.

heap LRU

> Política de Último Usado Recientemente (Last Recently Used) implementada usando un heap. Funciona como LRU, pero usa una pila (heap) en su lugar.

Nota

Si se utiliza la política LFUDA, el valor de *Tamaño máximo de objeto* debería incrementarse por encima de su por defecto de 4096 KB para maximizar el potencial de ratio de aciertos en bytes mejorado de LFUDA.

Política de reemplazo de caché. El parámetro de política de reemplazo de caché decide qué objetos se mantendrán en caché y cuáles serán evitados (reemplazados) para crear espacio para nuevos objetos. La política por defecto de reemplazo de caché en IPCop es LRU.

Ver más arriba para más detalles.

Activar modo offline. Activar esta opción desactivará la validación de objetos cacheados. Esto da acceso a más información cacheada (versiones obsoletas cacheadas, en las que el servidor original debería haber sido contactado).

No cachear estos destinos (opcional). Una lista de sitios que hará que la petición no se sirva desde la caché y que la respuesta no se cachee. En otras palabras, utilice esto para forzar objetos a que nunca sean cacheados.

Ejemplos:

Dominios completos y subdominios

```
*.ejemplo.net
*.google.com
```

Hosts únicos

```
www.ejemplo.net
www.google.com
```

Direcciones IP

```
81.169.145.75
74.125.39.103
```

URLs

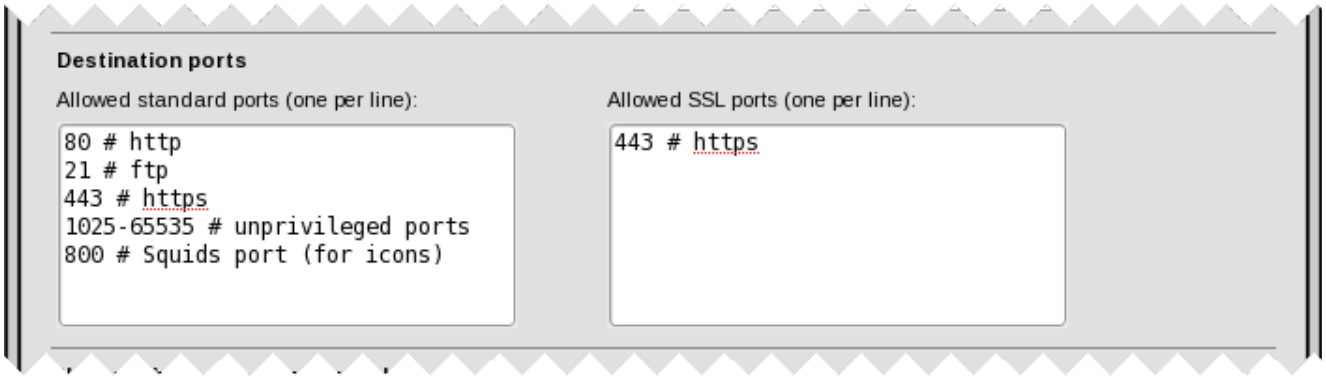
```
www.ejemplo.net/download
www.google.com/images
```

Nota

Puede introducir todos estos tipos de destino en cualquier orden.

2.5.1.6. Puertos de destino

Estos campos enumeran los puertos de destino permitidos para peticiones HTTP estándar y HTTPS encriptadas.



Los puertos se pueden definir como un solo número de puerto o como un rango de puertos.

Puertos estándar por defecto.

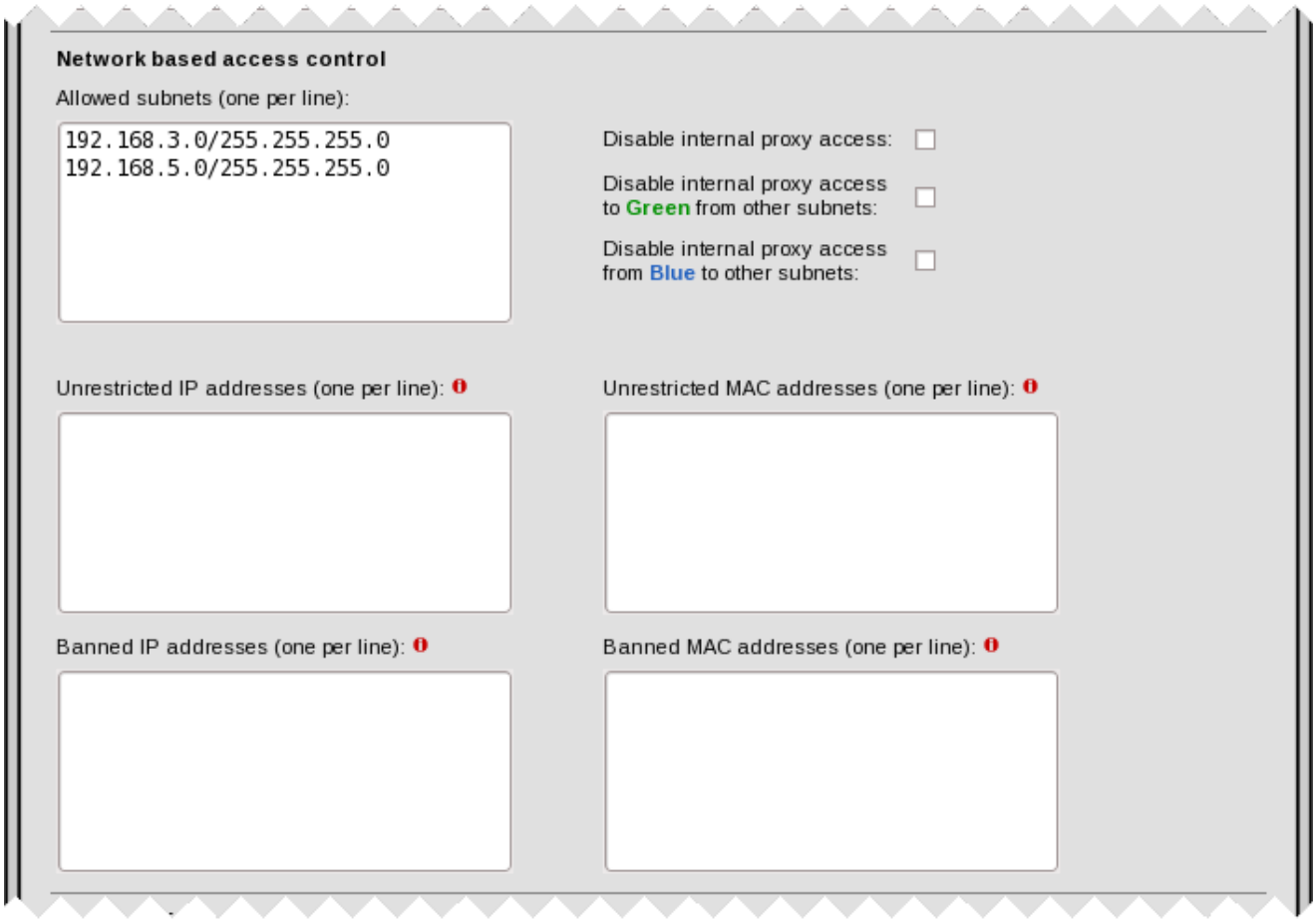
```
80 # http
21 # ftp
443 # https
1025-65535 # puertos sin registrar
800 # Puerto de squid (para iconos)
```

Puertos SSL por defecto.

```
443 # https
8443 # https alternativo
```

2.5.1.7. Control de acceso basado en red

Esto define el control de acceso para acceder al servidor proxy basándose en la dirección de red del cliente.



Subredes permitidas. Todas las subredes listadas tienen acceso al servidor proxy. Por defecto, las subredes VERDE y AZUL (si está disponible) están listadas aquí.

Puede añadir otras subredes, como subredes por detrás de VERDE en entornos grandes, a esta lista. Todas las redes *no* listadas aquí tendrán el acceso web bloqueado.

Desactivar acceso interno al proxy. Esta opción evita el acceso directo HTTP a través del servicio de proxy interno a servidores web locales en esas subredes, como se definieron más arriba. Esta selección prevalece sobre las siguientes dos opciones, que gestionan el acceso HTTP a VERDE y desde AZUL.

Desactivar el acceso interno por proxy a Verde desde otras subredes. Esto evita el acceso directo HTTP a través del servicio de proxy interno a servidores web en VERDE desde cualquier otra subred (p.e. AZUL).

Por ejemplo, cuando el acceso al proxy está activado para VERDE y AZUL, normalmente todas las peticiones se reenviarán a ROJA. Pero cuando un cliente de AZUL quiere acceder a un servidor web en VERDE, el servidor proxy toma el atajo interno entre la interfaz AZUL y la VERDE, independientemente de cualquier regla del cortafuegos.

Nota

Para proteger sus servidores en VERDE, se recomienda que active esta opción y utilice el Filtro de Direcciones o pinholes DMZ si es necesario.

Desactivar el acceso interno por proxy desde Azul a otras subredes. Esto evita el acceso directo HTTP a través del servicio de proxy interno desde AZUL a servidores web en cualquier otra subred (p.e. VERDE).

Por ejemplo, cuando el acceso al proxy está activado para VERDE y AZUL, normalmente todas las peticiones se reenviarán a ROJA. Pero cuando un cliente de AZUL quiere acceder a un servidor web en VERDE, el servidor proxy toma el atajo interno entre la interfaz AZUL y la VERDE, independientemente de cualquier regla del cortafuegos.

Nota

Esta opción está disponible sólo si hay una interfaz AZUL instalada.

Si está activado, los clientes en AZUL sólo pueden acceder a servidores web en AZUL o en ROJA.

Direcciones IP sin restricciones (opcional). Todas las direcciones IP de clientes en esta lista se saltarán las siguientes restricciones:

- Restricciones por horas
- Límites de tamaño para peticiones de descarga
- Capacidad de descarga
- Comprobación de navegador
- Filtro de tipos MIME
- Autenticación (por defecto, se requerirá para estas direcciones, pero se puede desactivar)
- Sesiones concurrentes por usuario (sólo disponible si la autenticación está activada)

Direcciones MAC sin restricciones (opcional). Todas las direcciones MAC de clientes en esta lista se saltarán las siguientes restricciones:

- Restricciones por horas
- Límites de tamaño para peticiones de descarga
- Capacidad de descarga
- Comprobación de navegador
- Filtro de tipos MIME
- Autenticación (por defecto, se requerirá para estas direcciones, pero se puede desactivar)
- Sesiones concurrentes por usuario (sólo disponible si la autenticación está activada)

Usar direcciones MAC en vez de direcciones IP puede ser útil si el servidor DHCP está activo y no tiene concesiones fijas definidas.

Las direcciones MAC pueden ser introducidas de cualquiera de estas dos formas:

```
00-00-00-00-00-00
00:00:00:00:00:00
```

Nota

El servidor proxy sólo puede determinar direcciones MAC de clientes configurados en las interfaces de las subredes VERDE, AZUL o NARANJA.

Direcciones IP prohibidas (opcional). Todas las peticiones de clientes (direcciones IP o subredes) en esta lista serán bloqueadas.

Direcciones MAC prohibidas (opcional). Todas las peticiones de clientes en esta lista serán bloqueadas.

2.5.1.8. Extensiones de Aula

Las Extensiones de Aula (EA) del servidor proxy le proporcionan la posibilidad de delegar tareas administrativas a usuarios no administrativos a través de una página de Gestión de Acceso Web separada.

Vea la sección Extensiones de Aula para más información.

2.5.1.9. Restricciones por horas

Esta sección define cuándo está activo el proxy web. La posición por defecto es permitir el acceso las 24 horas del día, 7 días a la semana.

La Opción de acceso “permitir” permite el acceso web, y la opción “denegar” bloquea el acceso web durante la franja de tiempo seleccionada. la elección entre “permitir” o “denegar” dependerá de las reglas horarias que quiera aplicar.

Las Restricciones por hora no afectarán a estos clientes:

- Direcciones IP sin restricciones
- Direcciones MAC sin restricciones
- Miembros del grupo “Extendido” si el proxy usa “Autenticación local”

2.5.1.10. Límite de transferencia

Esta sección le permite introducir límites al tamaño de cada petición de descarga y/o subida. Los valores vienen dados en Kilobytes (KB). Puede utilizar esto para evitar que sus usuarios descarguen archivos grandes y se ralentice el acceso a Internet para todos los demás.

Ponga los campos Tamaño máximo de descarga y Tamaño máximo de subida a 0, el valor por defecto, para eliminar todas las restricciones.

Los límites de descarga no afectarán a estos clientes:

- Direcciones IP sin restricciones
- Direcciones MAC sin restricciones
- Miembros del grupo “Extendido” si el proxy usa “Autenticación local”

2.5.1.11. Capacidad de descarga

El ancho de banda puede estar deslimitado, o limitado por interfaz, y/o por host, o basado en el tipo de contenido.

La capacidad de descarga no afectará a estos clientes:

- Direcciones IP sin restricciones
- Direcciones MAC sin restricciones

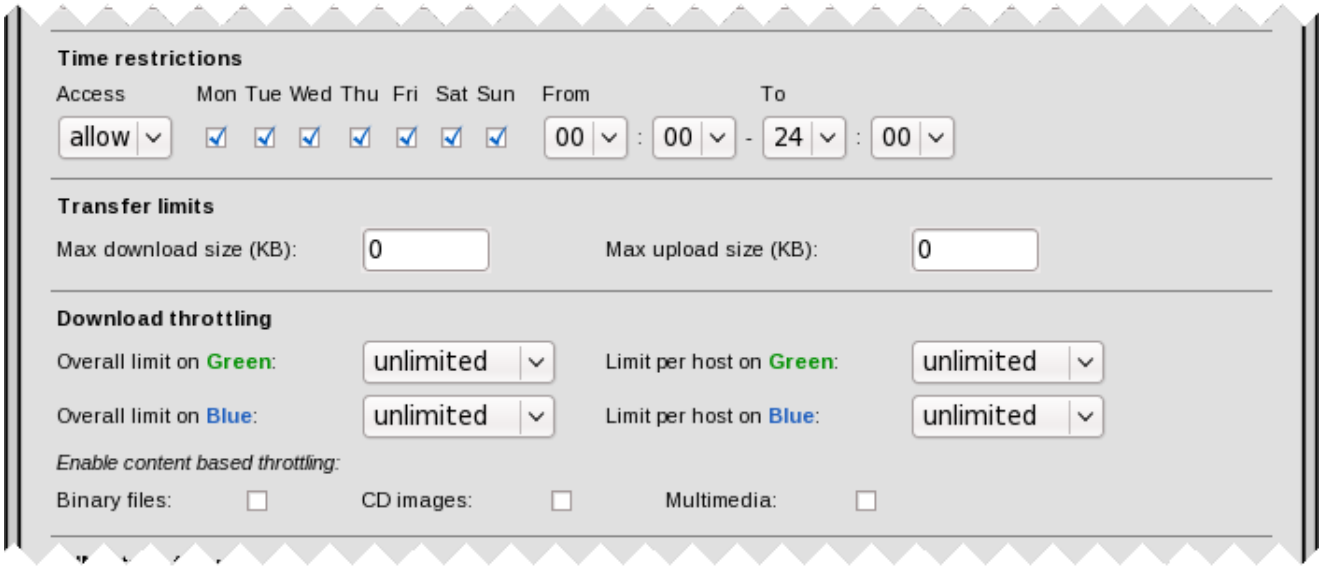
Los límites de ancho de banda se pueden definir por interfaz como un límite global, y por host. El ancho de banda usado por todos los hosts será limitado por el límite global.

Por defecto, los límites de ancho de banda afectan a todo tipo de tráfico, pero se puede limitar a ciertos tipos de contenido. De todas formas, esto desactiva el límite de ancho de banda para **otros** tipos de contenido.

El límite de ancho de banda por contenido se puede aplicar a:

- Archivos binarios: `bz2`, `bin`, `dmg`, `exe`, `sea`, `tar`, `tgz`, `zip` etc.
- Imágenes de CD: `ccd`, `cdi`, `img`, `iso`, `raw`, `tib` etc.
- Archivos multimedia: `aiff`, `avi`, `divx`, `mov`, `mp3`, `mp4`, `mpeg`, `qt` etc.

Figura 2.25. Proxy web - Secciones de Restricciones por hora, Límites de transferencia & Capacidad de descarga



2.5.1.12. Filtro de tipos MIME

El filtro de tipos MIME se puede configurar para bloquear contenidos dependiendo de su tipo MIME.

Activado. Si está activado, el filtro comprueba el tipo MIME en todas las cabeceras entrantes.

Bloquear estos tipos MIME (opcional). Si el tipo MIME solicitado está listado para ser bloqueado, se denegará el acceso al mismo. De esta manera puede bloquear contenido, sin importar el tipo de extensión de archivo utilizado.

Por ejemplo, añada este tipo MIME en una línea si quiere bloquear la descarga de archivos de Word:

```
application/msword
```

O añada estos tipos MIME, cada tipo en una línea, si quiere bloquear la descarga de archivos de video MPEG y QuickTime:

```
video/mpeg
video/quicktime
```

No filtrar estos destinos (opcional). Utilice esta lista para *evitar* el filtrado de tipos MIME sobre destinos concretos. Esto debe ser ser una lista, cada elemento en una línea, de dominios o subdominios, nombres de hosts, direcciones IP, o URLs.

Algunos ejemplos pueden ser:

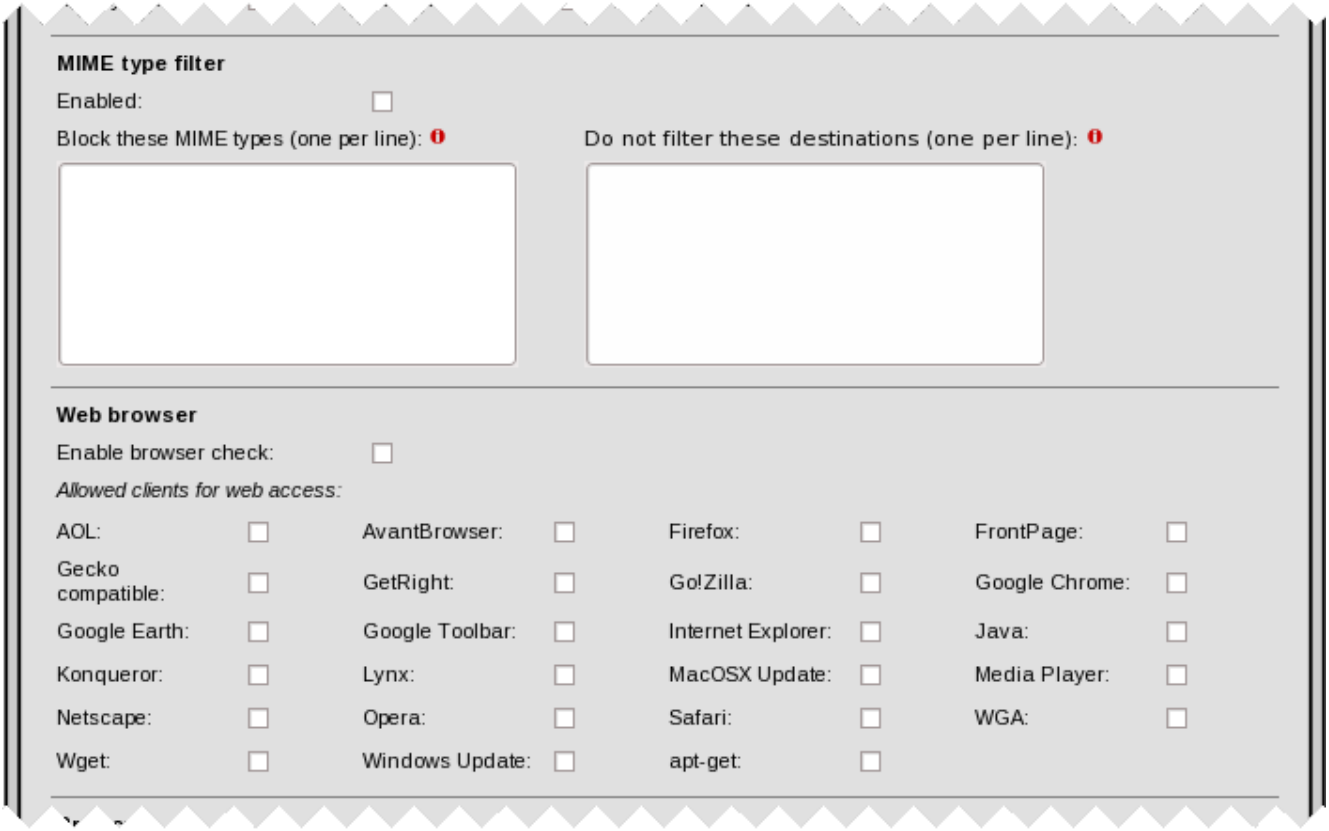
```
*.ejemplo.net
www.ejemplo.net
123.45.67.89
www.ejemplo.net/downloads
```

2.5.1.13. Navegador

Activar comprobación del navegador. Marque esta casilla si quiere activar la comprobación del navegador.

Clientes con acceso web permitido. Marque la(s) casilla(s) apropiada(s) para los clientes permitidos.

Figura 2.26. Proxy Web - Secciones Filtro de tipos MIME & Navegador



2.5.1.14. Privacidad

Esto permite la modificación de algunos campos de las cabeceras HTTP para proteger su privacidad.

'Useragent' falso enviado a sitios externos (opcional). Por defecto, se enviará el 'useragent' del navegador empleado a los servidores web externos. Algunos sitios dinámicos generan el contenido en función de la cadena 'useragent' enviada. Esta cadena también se anotará en los archivos de registro del servidor web.

Con la opción "'Useragent falso" tiene la posibilidad de reescribir esta cadena para todos sus clientes. Para las peticiones salientes, el campo de la cabecera 'useragent' será cambiado por el servidor proxy y enviado a los sitios externos en vez de la cadena 'useragent' original. Esto puede ser útil para proteger su privacidad o para forzar un nivel deseado de compatibilidad.

'Referrer' falso enviado a sitios externos (opcional). Cuando se pulsa sobre un enlace, la URL de origen se enviará al sitio web de destino. Esto se puede desactivar introduciendo una cadena definida por el usuario. Esta cadena será la enviada en vez de la URL de referencia original. Esto puede ser útil para proteger su privacidad.

Nota

Modificar el 'referrer' viola el estándar HTTP y a veces puede llevar a dificultades. Algunos sitios web bloquean las peticiones con un 'referrer' no válido para protegerse contra los llamados enlaces profundos (deep links) o el abuso de "robar" gráficos de su sitio web.

2.5.1.15. Redireccionadores

Los redireccionadores trabajan con el proxy para filtrar y redireccionar el tráfico web basándose en reglas que pueden incluir listas negras, listas blancas, franjas horarias, etc.

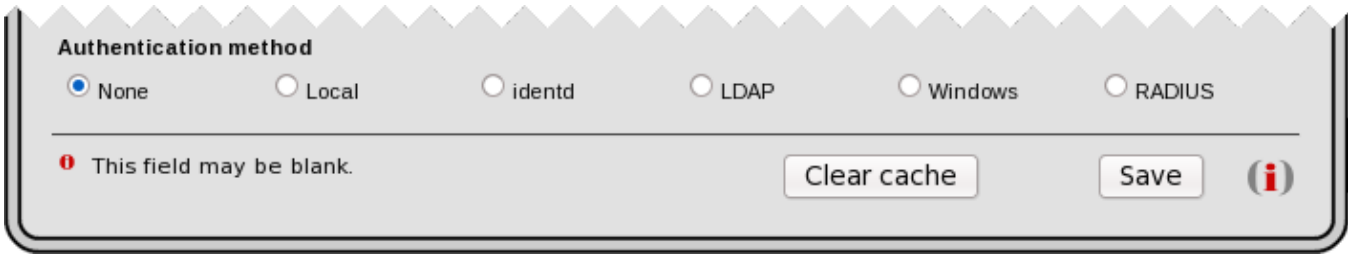
Activado. Marque la casilla para activar los redireccionadores.

Número de procesos de redirección. Puede incrementar o disminuir el número de procesos activos de filtrado. El número de procesos depende de las prestaciones de su hardware, su ancho de banda y el número de clientes concurrentes. El valor por defecto es 5.

Redirectores disponibles. Lista los redirectores instalados y cuáles están activos. *URL Filter*, en este ejemplo.

2.5.1.16. Método de autenticación

El Proxy web ofrece varios métodos para la autenticación de usuarios.



Ninguno (por defecto). La autenticación está desactivada. Los usuarios no necesitan autenticarse para acceder a sitios web.

Local. Este metodo de autenticación es el más adecuado para entornos SOHO. Los usuarios necesitan autenticarse cuando accedan a sitios web introduciendo un nombre de usuario y contraseña válidos. Vea la sección Autenticación Local del Proxy para más información.

identd. Este método de autenticación es el más adecuado en entornos donde:

- La autenticación tiene que ser un proceso "oculto" sin introducir nombre de usuario y contraseña.
- El servicio de proxy debe operar en modo transparente.
- Los nombres de usuario sólo se utilizarán para registro y no para autenticación.

El método de autenticación identd requiere un servicio o demonio **identd** corriendo en el cliente. Vea la sección Autenticación identd para más información.

LDAP. Este método de autenticación es el más adecuado en entornos de red medios y grandes. Los usuarios se tendrán que autenticar cuando accedan a sitios web entrando un nombre de usuario y contraseña válidos. Las credenciales son verificadas contra un servidor externo usando el Protocolo Ligero de Acceso a Directorios (LDAP).

La autenticación LDAP es útil si ya tiene un servicio de directorio en su red y no quiere mantener cuentas de usuario y contraseñas adicionales para el acceso web. Vea la sección Autenticación LDAP para más información.

Windows. Este método de autenticación es adecuado para entornos de red pequeños y medianos. Los usuarios tienen que autenticarse cuando acceden a sitios web. Las credenciales se verifican contra un servidor externo que actúa como Controlador de Dominio. Vea la sección Autenticación Windows para más información.

RADIUS. Este método de autenticación es adecuado para entornos de red pequeños y medianos. Los usuarios tienen que autenticarse cuando acceden a sitios web. Las credenciales se verifican contra un servidor RADIUS externo. Vea la sección Autenticación RADIUS para más información.

Nota

Cuando se utilice autenticación y estén activos los archivos de registro del proxy web, se registrará el nombre de usuario requerido además de la URL solicitada. Antes de activar el registro cuando utilice autenticación, asegúrese de no violar las leyes existentes.

2.5.1.17. Limpiar caché/Guardar

Limpiar caché. Puede eliminar todas las páginas de la caché del proxy en cualquier momento pulsando el botón Limpiar caché.

Guardar. Tras realizar cualquier cambio, pulse el botón Guardar para aplicarlo.

2.5.2. Página administrativa de URL Filter

URL filter amplía la funcionalidad de IPCop con la capacidad de bloquear accesos a dominios, URLs y archivos no deseados. Esta prestación está basada en el conocido redirector squidGuard. La interfaz gráfica de usuario de URL filter le proporciona acceso a todos los ajustes requeridos, incluyendo las listas negras compatibles con squidGuard, y restricciones basadas en horas, categorías y clientes.

URL filter fue originalmente escrito por Marco Sondermann como un 'add-on' para IPCop. Se incluyó en la versión v2.1.1 de IPCop.

2.5.2.1. URL Filter

La primera línea en la sección de Ajustes indica si el servicio de filtrado está parado o corriendo.

2.5.2.2. Ajustes comunes

Activado. Esta casilla tiene que estar marcada para activar URL Filter. Además, URL Filter tiene que estar activado en la página del Proxy Web.

Registro activado. Active esto para escribir a un archivo de registro todas las peticiones ofensivas.

Registrar nombre de usuario. Active esto para añadir el nombre de usuario para cada petición en el archivo de registro.

Partir el registro por categorías. Divide el archivo de registro en archivos individuales, uno por cada categoría en vez de un archivo de registro común. La opción Registro activado tiene que estar activa.

2.5.2.3. Categorías bloqueadas

Se pueden seleccionar diferentes categorías, en función de las listas negras instaladas.

2.5.2.4. Lista negra/blanca/de expresiones personalizadas

Lista negra personalizada - Activada. Active esto para bloquear dominios y URLs introducidos manualmente.

Dominios bloqueados (uno por línea) opcional. Defina los dominios que quiere bloquear. Éstos podrian ser:

```
ejemplo.net
subdominio.ejemplo.net
```

URLs bloqueadas(una por línea) opcional. Defina las URLs que quiere bloquear. Éstas podrian ser:

```
ejemplo.net/foo
ejemplo.net/foo/bar
```

Lista blanca personalizada - Activada. Active esto para permitir dominios y URLs introducidas manualmente, incluso aunque estén listadas en otra categoría.

Dominios permitidos (uno por línea) opcional. Defina los dominios que quiere permitir. Éstos podrian ser:

```
ejemplo.net
subdominio.ejemplo.net
```

URLs permitidas(una por línea) opcional. Defina las URLs que quiere permitir. Éstas podrían ser:

```
ejemplo.net/foo
ejemplo.net/foo/bar
```

Lista de Expresiones personalizada - Activada. Hace que las URLs sean bloqueadas si la expresión introducida manualmente coincide con ellas.

Expresiones bloqueadas (como expresiones regulares) opcional. Defina las expresiones a bloquear si aparecen en una URL. Puede emplear expresiones regulares para esto, una por línea.

2.5.2.5. Bloqueo de extensiones de archivo

Archivos binarios. Active esto para bloquear la descarga de archivos ejecutables. Esto incluye archivos calificados como potencialmente inseguros. Algunas extensiones son:

```
.bat .com .exe .sys .vbs
```

Multimedia. Active esto para bloquear la descarga de archivos relacionados con audio y video. Ejemplos de extensiones de archivos multimedia son:

```
.aiff .avi .dif .divx .mov .movie .mp3 .mpeg .mpv2 .ogg .qt .wav .wma .wmf .wmv
```

Archivos comprimidos. Active esto para bloquear la descarga de archivos comprimidos conteniendo otros archivos. Ejemplos de extensiones de archivos comprimidos son:

```
.bin .bz2 .cab .cdr .dmg .gz .hqx .rar .sit .sea .tgz .zip
```

2.5.2.6. Control de acceso basado en red

Direcciones IP sin restricciones (opcional). La(s) dirección(es) IP o red(es) listadas se saltarán todas las reglas de filtrado activas.

Direcciones IP prohibidas (opcional). La(s) dirección(es) IP o red(es) listadas serán prohibidas, independientemente de las reglas de filtrado activas.

Puede definir una o más direcciones de hosts individuales, redes en notación CIDR, redes con una máscara de red concreta, un rango de hosts, o una combinación de todos ellos.

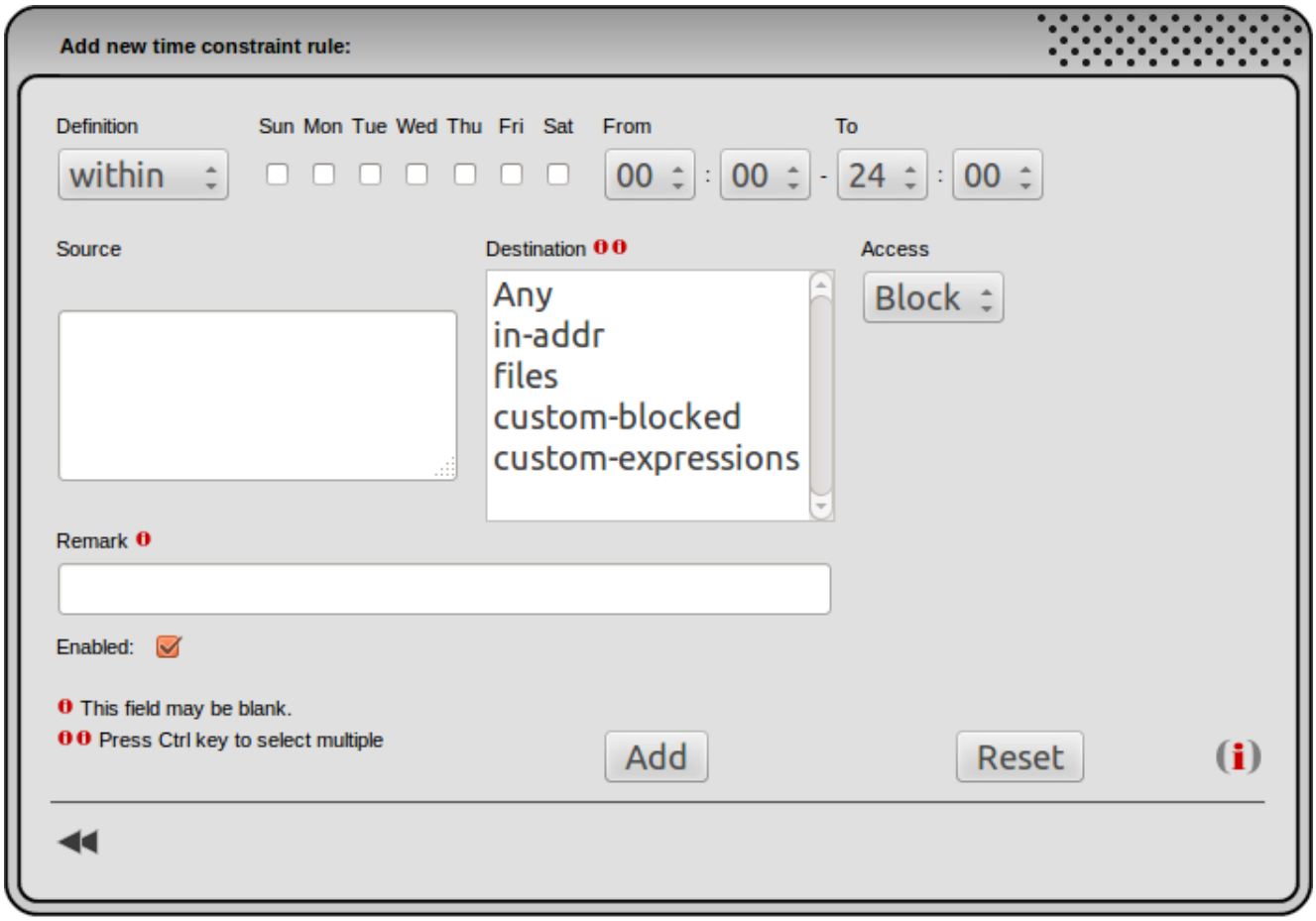
Algunos ejemplos son:

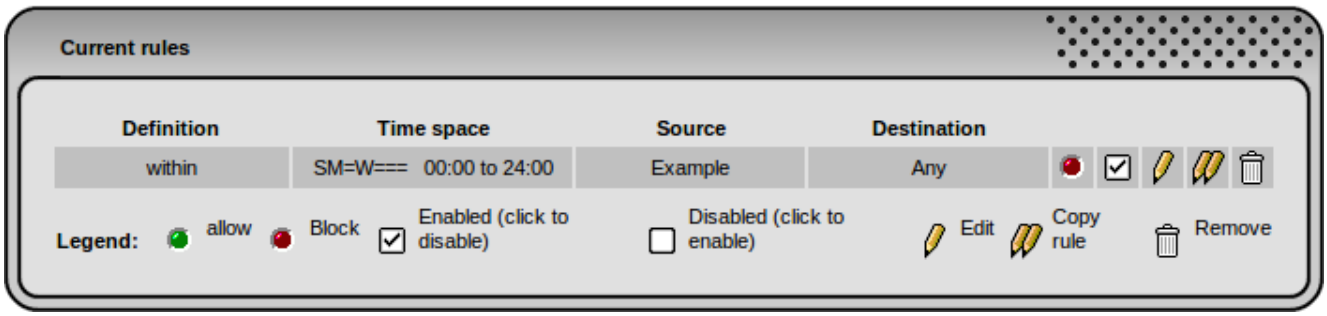
```
192.168.0.54
192.168.0.0/24
192.168.0.0/255.255.255.0
192.168.0.100-192.168.0.200
```

2.5.2.7. Control de acceso basado en horas

Hay dos botones en esta sección. Ajustar restricción por horas abre otro diálogo GUI para restricciones basadas en horas, y Ajustar cuota de usuario abre un diálogo GUI para cuotas horarias basadas en usuario.

El primer botón le lleva a un diálogo que le permite añadir y editar reglas de restricción por horas. Las reglas actuales se muestran al pie de la página.





Definición. Determina si la regla estará activa *dentro* o *fuera* del marco de tiempo dado.

Día de la semana. Seleccione los días de la semana de Lunes a Domingo para la regla.

Desde/hasta. Horas de inicio y fin para la regla. Nota: ¡La hora se refiere a la hora de URL filter y no a la hora del cliente local!

Origen. Introduzca el host o la(s) dirección(es) de red de origen para la regla.

Destino. Seleccione una o más categorías. Para seleccionar más de una categoría, presione la tecla Ctrl y pinche sobre la categoría deseada.

Además de las categorías regulares de bloqueo, hay cuatro categorías más:

```
cualquiera : incluye todas las categorías
en-dirección : incluye todas las URLs accedidas por su dirección IP
archivos : incluye todos los bloqueos de extensiones de archivos
bloqueos-personalizados : incluye las listas negras personalizadas de dominios y
URLs
```

Estas categorías se pueden seleccionar, aunque no estén activadas en la página principal.

Acceso. Determina si la regla permitirá o bloqueará el acceso.

Activada. Activa la regla.

Añadir/Actualizar. Guarda la regla. Nota: ¡URL filter necesita ser reiniciado para activar los cambios!

Descartar. Descarta todos los cambios para la regla actual y relee los ajustes guardados.

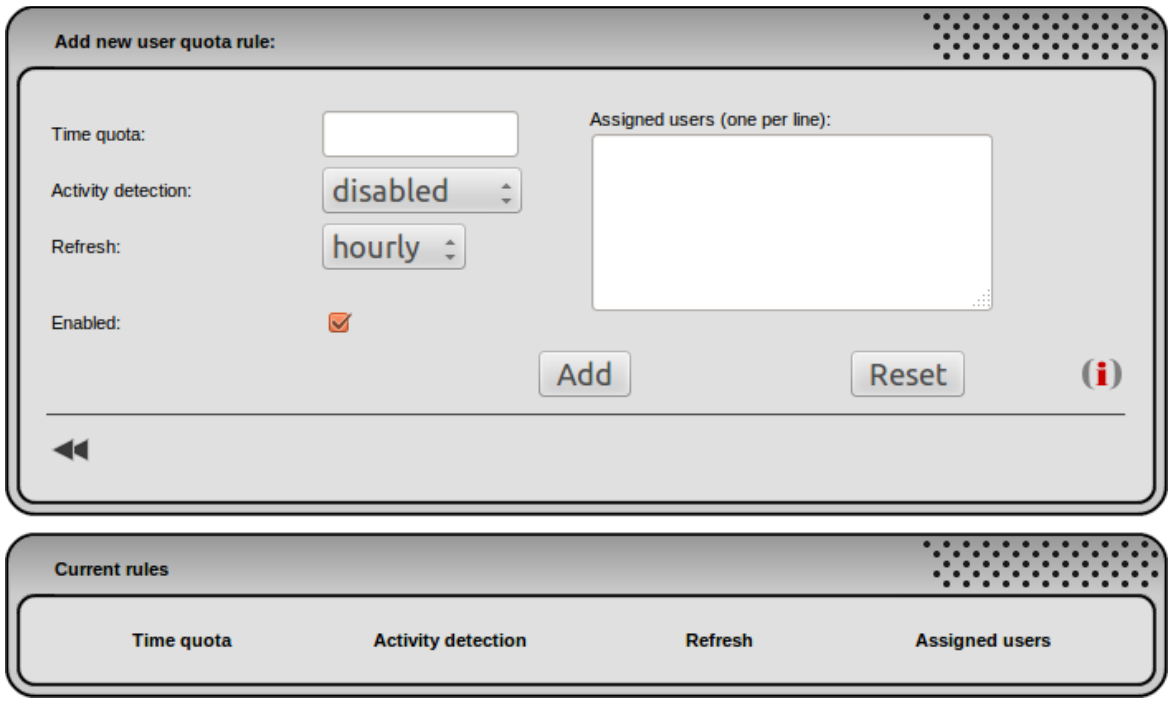
<<. Vuelve a la página principal de URL Filter.

Reglas actuales. Muestra todas las reglas de restricción por horas.

Nota

¡Todas las reglas se aplican en el mismo orden en el que están listadas!

El botón Ajustar cuota de usuario le lleva a un diálogo que le permite añadir y editar reglas de cuota horaria por usuario. Las reglas actuales se muestran al pie de la página.



Cuota horaria. El tiempo (en minutos) que un usuario puede tener acceso a la web. El contador se inicia con la primera petición y el usuario es bloqueado si se alcanza este límite de tiempo.

Detección de actividad. Si el usuario no accede a ningún sitio web durante 5 o 15 minutos, el límite de cuota no disminuirá hasta que se envíe la siguiente petición.

Refrescar. Especifica el marco de tiempo para la cuota de usuario dada. La cuota para este usuario se reiniciará cada hora, cada día o cada semana.

Usuarios asignados. Los nombres de usuario según RFC931 que serán afectados por esta regla.

Activada. Activa la regla.

Añadir/Actualizar. Guarda la regla. Nota: ¡URL filter necesita ser reiniciado para activar los cambios!

Descartar. Descarta todos los cambios para la regla actual y relee los ajustes guardados.

<<. Vuelve a la página principal de URL Filter.

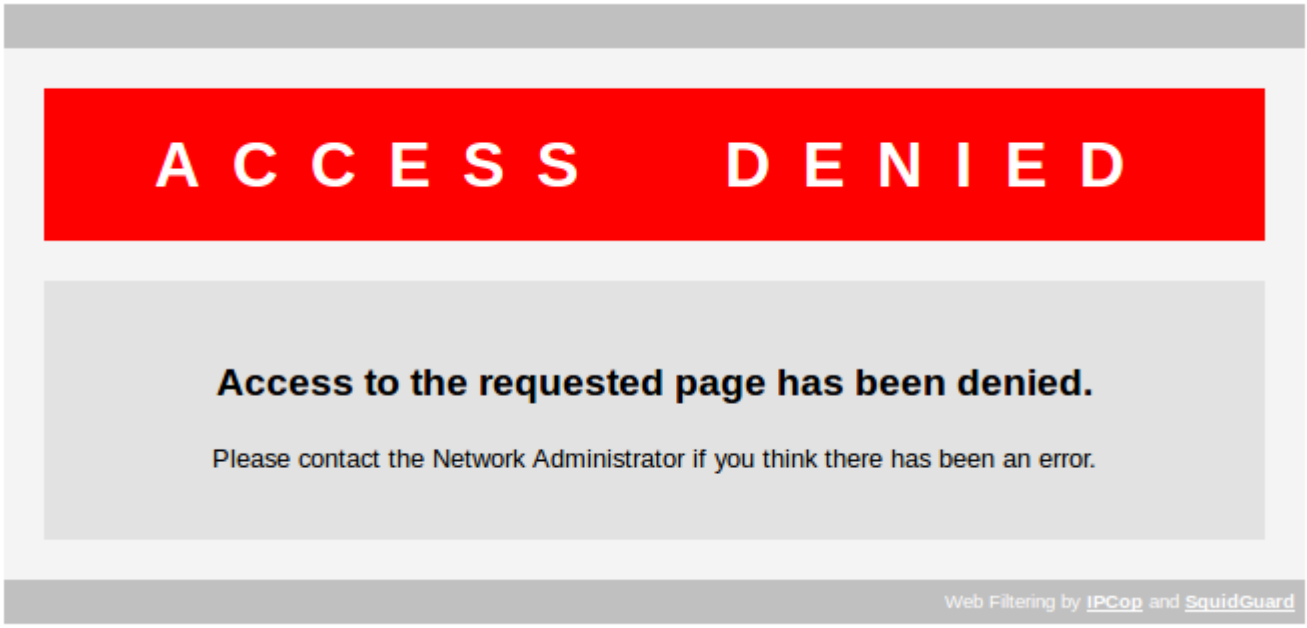
Reglas actuales. Muestra todas las reglas de restricción horaria existentes.

Nota

¡Los contadores de cuota actuales se reiniciarán para todos los usuarios cuando se reinicie URL filter, el servicio de proxy o el servidor!

2.5.2.8. Ajustes de la página de bloqueo

Cuando un cliente intenta visitar una página web en la lista de bloqueos, es redireccionado a la “Página de bloqueo” mostrada más abajo. El contenido de la Página de bloqueo puede ser personalizado cambiando varios ajustes.



Mostrar categoría en página de bloqueo. Si está activado, la categoría se mostrará en el mensaje de bloqueo. Esto puede ser una indicación útil si no está seguro de qué categoría está bloqueando su petición.

Mostrar URL en página de bloqueo. Si está activado, la URL solicitada se mostrará en el mensaje de bloqueo.

Mostrar IP en página de bloqueo. Si está activado, la dirección IP del cliente se mostrará en el mensaje de bloqueo.

Usar Error DNS para URLs bloqueadas. El mensaje de bloqueo por defecto será reemplazado por un mensaje de "Error de servidor o DNS no encontrado". Esto puede ser útil cuando quiere que el destino se muestre a los clientes como caído, en vez de bloqueado. Esta opción sólo debe ser utilizada con el servicio de Proxy Web corriendo en modo transparente.

Activar inagen de fondo. Si está activado, se mostrará una imagen de fondo en la página de bloqueo. La imagen por defecto es el logo de IPCop.

La imagen de fondo puede ser reemplazada por su propia imagen personalizada, si coloca un archivo gráfico .png en IPCop, en este directorio y con este nombre de archivo:

`/home/httpd/html/images/custom-redirect-background.png`

Redirigir a esta URL (opcional). Puede definir un sitio web personalizado al que los clientes serán redirigidos si son bloqueados.

Línea de mensaje 1 (opcional). Puede definir su propio texto aquí para reemplazar el texto por defecto "ACCESO DENEGADO" en la página de bloqueo.

Línea de mensaje 2 (opcional). Puede definir su propio texto aquí para reemplazar el texto por defecto "El acceso a la página solicitada ha sido denegado" en la página de bloqueo.

Línea de mensaje 3 (opcional). Puede definir su propio texto aquí para reemplazar el texto por defecto "Por favor, contacte con su Administrador si cree que esto es un error" en la página de bloqueo.

Recuerde Guardar y reiniciar el servicio tras realizar cualquier cambio.

2.5.2.9. Ajustes avanzados

Activar listas de expresiones. Activa las listas de extensiones predefinidas. Además de las listas de dominios y URLs, se buscarán ciertas palabras clave en todas las URLs. La existencia de esas expresiones depende de la lista negra instalada.

Activar SafeSearch. Activa el filtrado SafeSearch, basado en motor de búsqueda, para la búsqueda de imágenes y la búsqueda web ordinaria. Esto puede depender de si el motor de búsqueda soporta la prestación SafeSearch.

Bloquear sitios accedidos por su dirección IP. Si está activado, todos los sitios accedidos por su dirección IP serán bloqueados. Los mismos sitios estarán disponibles si son accedidos por su nombre de dominio y no están por otra regla.

Bloquear "ads" con ventana vacía. Activar esto reemplaza los banners, las ventanas emergentes y los anuncios con una ventana en blanco. Esto se hace redireccionando a un archivo .gif de 1 pixel de tamaño. Requiere que la categoría “ads” o “adv” estén seleccionadas para bloquear.

Bloquear todas las URLs no permitidas explícitamente. Active esto para bloquear todas las peticiones, excepto aquellas definidas en la “Lista blanca personalizada”.

Permitir lista blanca personalizada para clientes prohibidos. Todas las peticiones de clientes prohibidos (prohibidos por definición o por restricciones horarias) serán bloqueadas por defecto. Si está activada, esta opción permite que los clientes prohibidos soliciten sitios web de la lista blanca. La lista blanca tiene que estar activada para esto.

2.5.2.10. Guardar/Guardar y reiniciar

Guardar. Tras realizar cualquier cambio, pulse el botón Guardar para guardarlo.

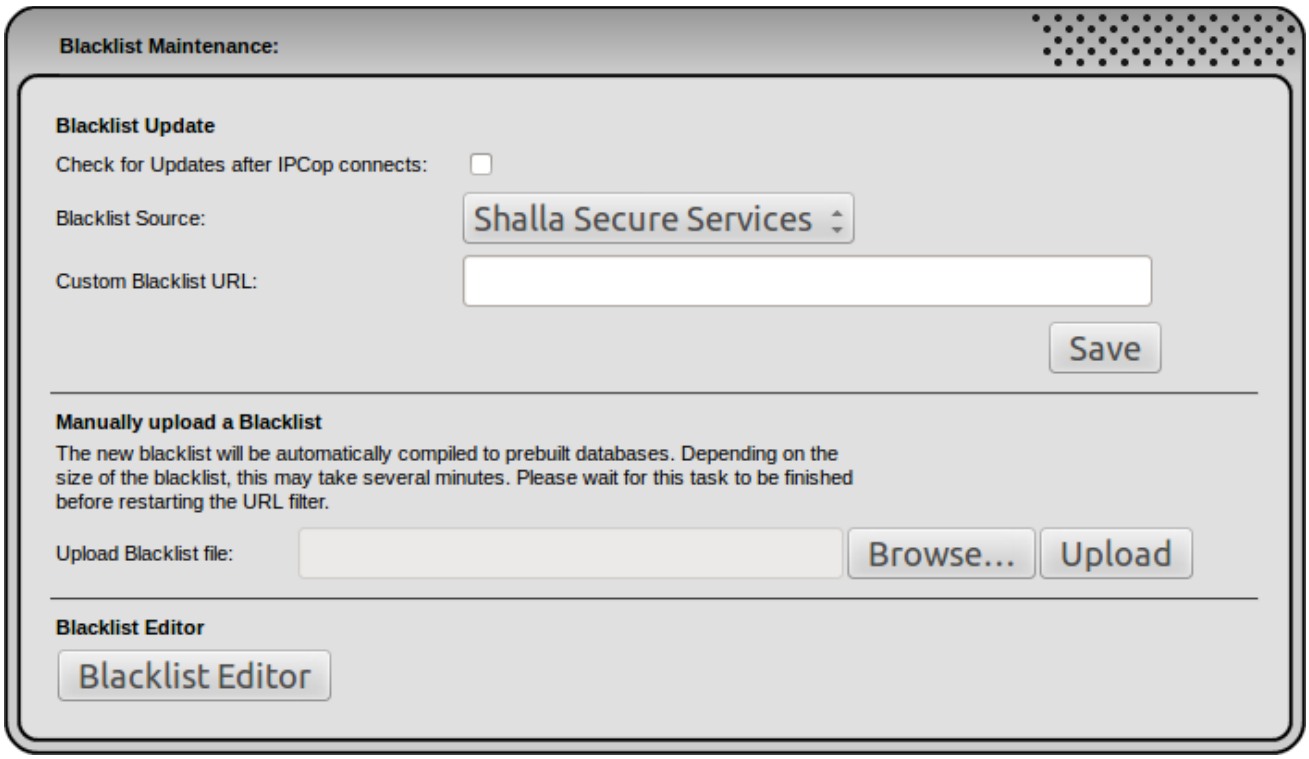
Guardar y reiniciar. Utilice el botón Guardar y reiniciar para guardar y aplicar los cambios.

2.5.2.11. Mantenimiento de la lista negra

Cualquier lista negra compatible con squidGuard se puede instalar con URL filter. Si instala una nueva lista negra, todas las categorías existentes se reemplazarán y se añadirán las nuevas categorías.

El archivo `.tar.gz` debe tener la ruta interna `blacklists/category/list`, donde `category` será el nombre de la categoría y `list` será uno o más archivos llamados `domains, urls` o `expressions`.

Dependiendo de las prestaciones de su hardware (especialmente su disco duro) y el tamaño de la lista negra, compilar la lista negra a bases de datos preconstruidas puede llevar varios minutos. Las bases de datos preconstruidas son necesarias para acelerar el proceso de inicio de URL filter de forma significativa, especialmente en máquinas con un bajo nivel de prestaciones.



Actualización de lista negra. Se pueden programar actualizaciones de la lista negra en la sección Programador.

Comprobar actualizaciones cuando IPCop se conecte es una opción que, cuando está activada, hace que se busque una actualización de la lista negra cuando IPCop se conecta a Internet.

Origen de la lista negra Seleccione una de las fuentes de descarga predefinidas, o una URL personalizada para la descarga.

Si selecciona una URL personalizada como fuente de descarga, introduzca la URL completa para la descarga en el campo URL personalizada de lista negra.

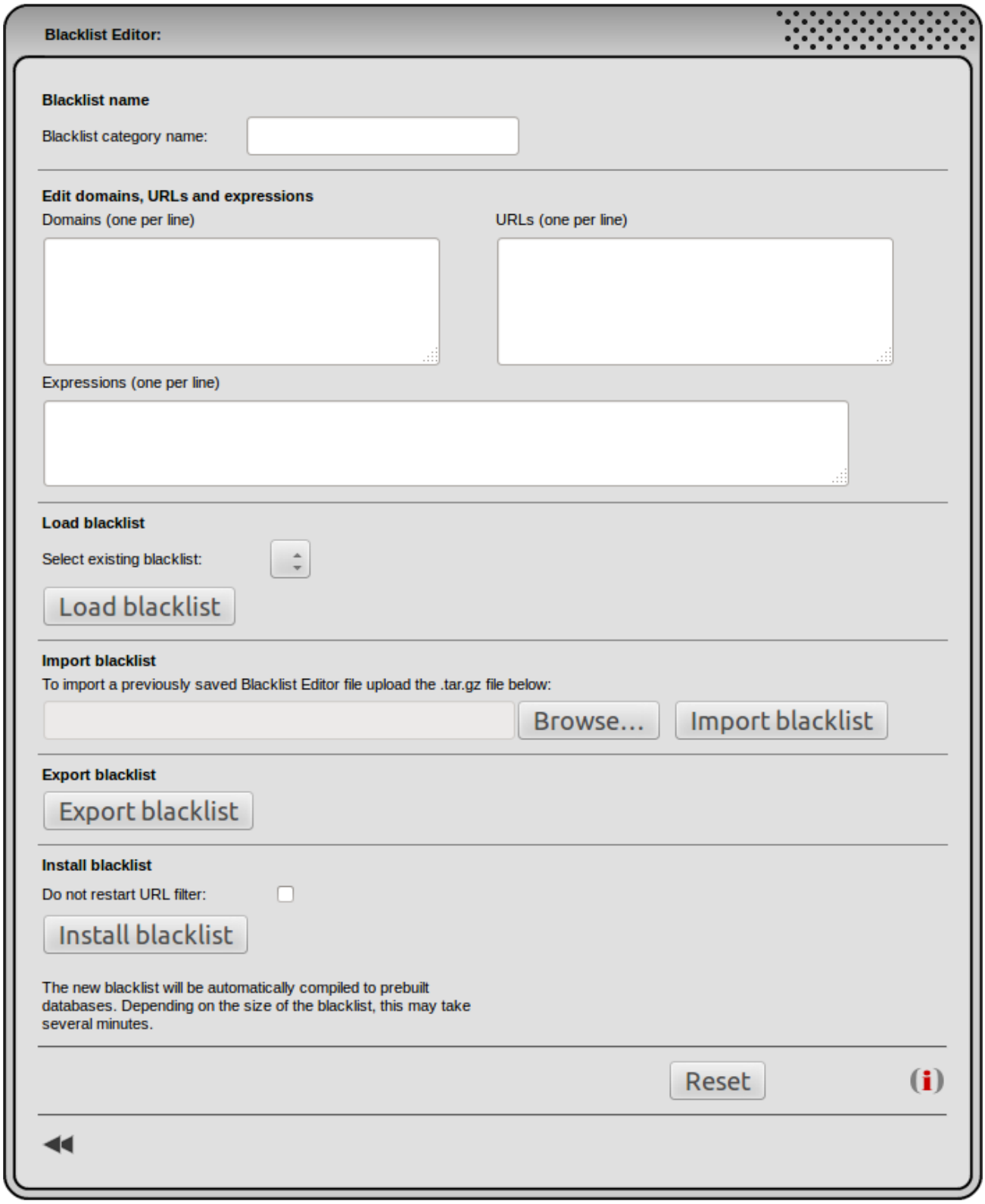
Tras realizar cualquier cambio, pulse el botón Guardar para guardarlo.

Subir una lista negra manualmente. Si tiene un archivo de lista negra compatible con squidGuard o una copia de seguridad de la lista negra instalada en su IPCop, puede subir el archivo en esta sección. El archivo será subido al servidor IPCop y compilado para su uso por URL filter.

Editor de lista negra. Vea la siguiente sección.

2.5.2.12. Editor de lista negra

Escribir introducción...



Nombre de la lista negra. Escribir sección...

Editar dominios, URLs y expresiones. Escribir sección...

Cargar lista negra. Escribir sección...

Importar lista negra. Escribir sección...

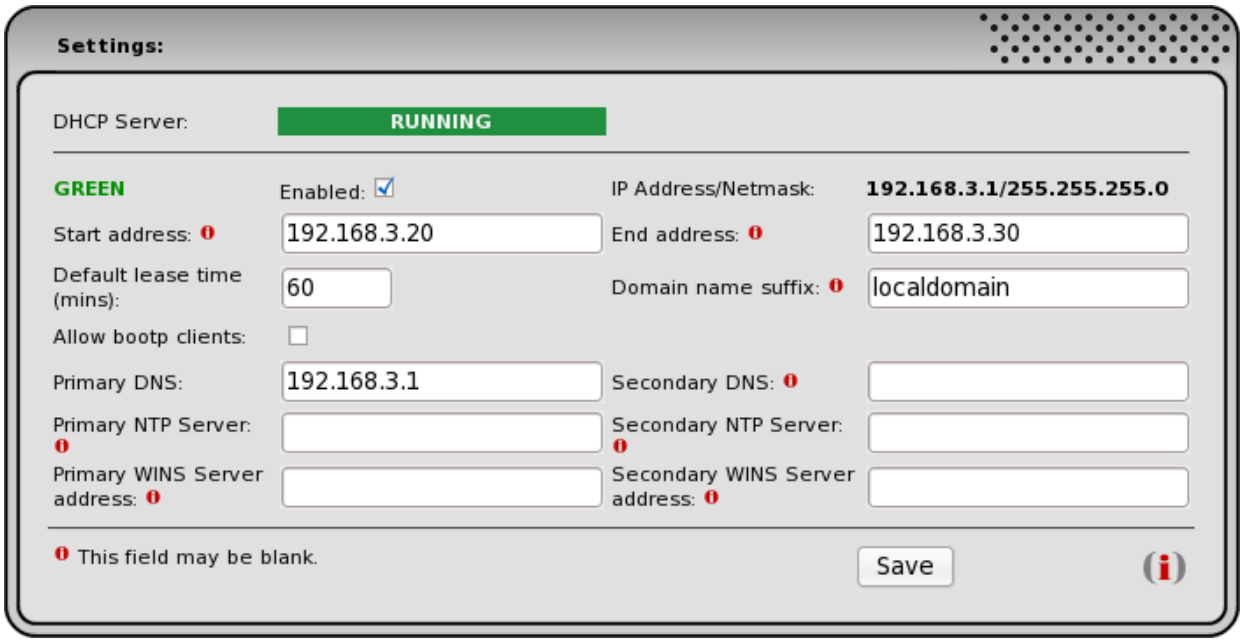
Exportar lista negra. Escribir sección...

Instalar lista negra. Escribir sección...

2.5.3. Página administrativa de DHCP

DHCP (Dynamic Host Configuration Protocol) le permite controlar la configuración de red de todos sus ordenadores o dispositivos desde su máquina IPCop. Cuando un ordenador (o un dispositivo como una impresora, pda, etc.) se une a su red, obtendrá una dirección IP válida y su configuración DNS y WINS será dada desde la máquina IPCop. Para utilizar esta prestación, las nuevas máquinas deben estar configuradas para obtener su configuración de red de forma automática.

Figura 2.27. Ajustes de DHCP



Puede elegir si quiere proporcionar este servicio a su red Verde y/o a su red Azul (si está instalada). Tan sólo marque la casilla correspondiente.

2.5.3.1. Parámetros del servidor DHCP

Los siguientes parámetros DHCP se pueden ajustar desde la interfaz web:

Activado. Marque esta casilla para activar el servidor DHCP para esta interfaz.

Dirección IP/Máscara de red. La dirección IP de la interfaz de red y su máscara de red se muestran aquí como referencia.

Dirección inicial (opcional). Puede especificar la dirección menor y mayor que el servidor manejará para los solicitantes. Si tiene máquinas en su red que no emplean DHCP, y tienen sus direcciones IP asignadas manualmente, debe ajustar las direcciones de inicio y final para que el servidor no maneje ninguna de esas IPs manuales.

Debería asegurarse también de que todas las direcciones listadas en la sección concesiones fijas (ver más abajo) están también fuera de este rango.

Dirección final (opcional). Especifica la dirección más alta que manejará (ver más arriba).

Nota

Para hacer que DHCP proporcione concesiones fijas sin manejar concesiones dinámicas, deje los dos campos, Dirección inicial y final, en blanco. De todas formas, si proporciona una dirección inicial, también tendrá que proporcionar una dirección final, y viceversa.

Tiempo de concesión por defecto. Esto se puede dejar con su valor por defecto a menos que necesite especificar su propio valor. El tiempo de concesión por defecto es el intervalo de tiempo durante el cual las concesiones son válidas. Antes de que el tiempo de concesión de una dirección expire, sus ordenadores solicitarán la renovación de su concesión, especificando su dirección IP actual. Si los parámetros DHCP se han cambiado, cuando se hace una solicitud de renovación los cambios se propagarán. Generalmente, las concesiones son renovadas por el servidor.

Sufijo de nombre de dominio (opcional). No debe haber un punto al inicio de esta casilla. Introduzca el nombre de dominio que el servidor DHCP pasará a los clientes. Si no se puede resolver algún nombre de host, el cliente lo intentará de nuevo tras añadir el nombre especificado al nombre de host original. Muchos servidores DHCP de ISPs ponen el nombre de su propia red como por defecto e indican a los clientes que introduzcan “www” como página por defecto en su navegador para acceder a la web. “www” no es un FQDN (fully qualified domain name). Pero el software de su ordenador añadirá el sufijo de nombre de dominio proporcionado por el servidor DHCP del ISP, creando un FQDN para el servidor web. Si no quiere que sus usuarios tengan que usar direcciones como 'www', ponga el sufijo de nombre de dominio de forma idéntica a como especifique el servidor DHCP del ISP.

Permitir clientes bootp. Marque esta casilla para hacer que los clientes bootp obtengan concesiones para su interfaz de red. Por defecto, el servidor DHCP de IPCop ignora los paquetes de solicitud Bootstrap (BOOTP).

DNS Primario. Especifica qué debe decir el servidor DHCP a sus clientes para usar como servidor DNS primario. Como IPCop corre un proxy DNS, probablemente quiera dejar el por defecto para que el servidor DNS primario sea la dirección IP de la máquina IPCop. Si tiene su propio servidor DNS, especifíquelo aquí.

DNS Secundario (opcional). También puede especificar un segundo servidor DNS que se usará si el primario no está disponible. Éste puede ser otro servidor DNS en su red o el de su ISP.

Servidor NTP Primario (opcional). Si está usando IPCop como servidor NTP, o quiere pasar la dirección de otro servidor NTP a los dispositivos de su red, puede poner su dirección IP en esta casilla. El servidor DHCP pasará esta dirección a todos los clientes cuando reciban los parámetros de red.

Servidor NTP Secundario (opcional). Si tiene un segundo servidor NTP, póngalo en esta casilla. El servidor DHCP pasará esta dirección a todos los clientes cuando reciban los parámetros de red.

Dirección del servidor WINS Primario (opcional). Si está corriendo una red Windows y tiene un servidor WINS (Windows Naming Service), puede poner su dirección IP en esta casilla. If you are running a Windows network and have a Windows Naming Service (WINS) server, you can put its IP address in this box. El servidor DHCP pasará esta dirección a todos los clientes cuando reciban los parámetros de red.

Dirección del servidor WINS Secundario (opcional). Si tiene un segundo servidor WINS, puede poner su dirección IP en esta casilla. El servidor DHCP pasará esta dirección a todos los clientes cuando reciban los parámetros de red.

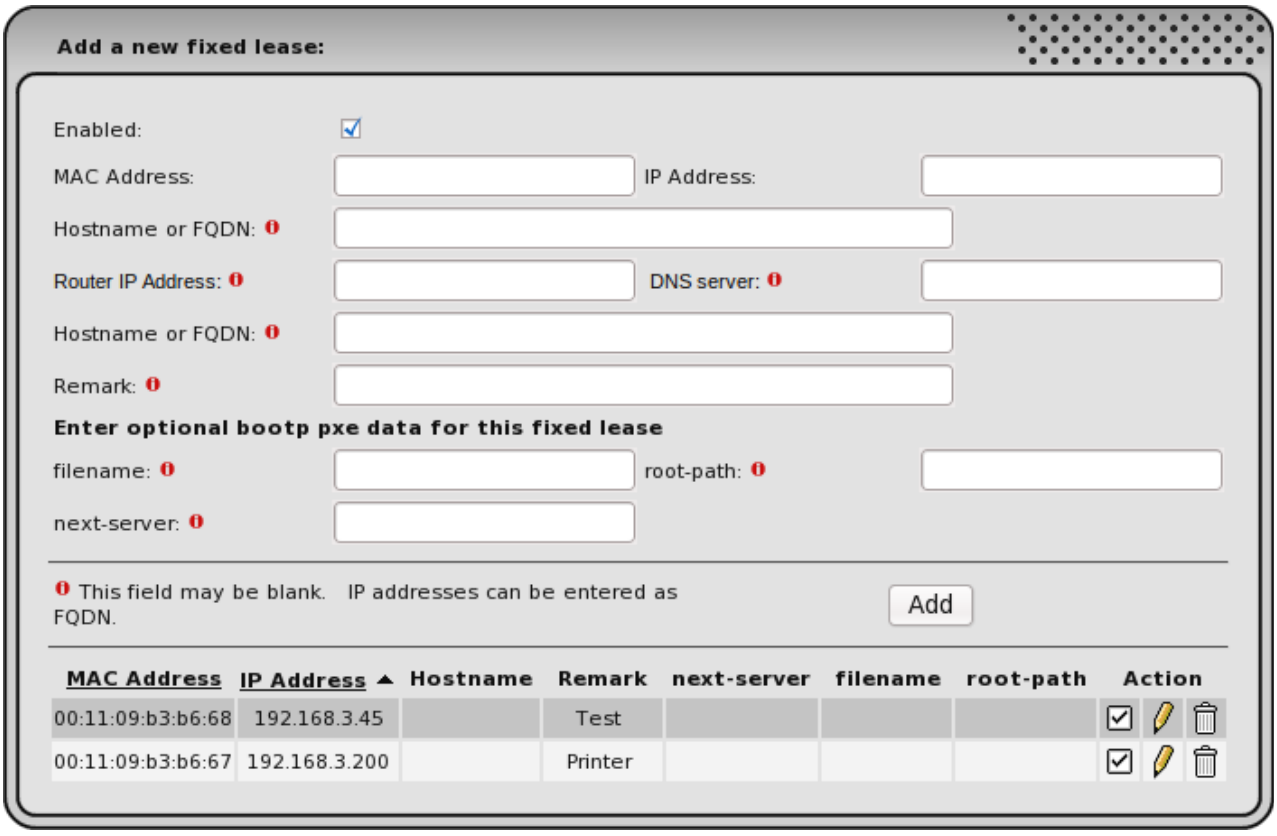
Cuando pulse Guardar, el cambio tendrá efecto.

2.5.3.2. Concesiones fijas

Si tiene máquina cuyas direcciones IP quiere gestionar de forma centralizada, pero necesitan tener siempre la misma direcció IP, puede decirle al servidor DHCP que asigne una dirección IP "estática", o "fija", basada en la dirección MAC de la tarjeta de red de la máquina, o en el nombre de host de la máquina.

Esto es diferente a utilizar direcciones manuales, ya que estas máquinas contactarán al servidor DHCP para solicitar su dirección IP y tomarán la que esté configurada para ellas.

Figura 2.28. Añadir una concesión fija



Puede especificar los siguientes parámetros para una concesión fija:

Activada. Marque esta casilla para decirle al servidor DHCP que maneje esta concesión fija. Si la entrada no está activada, será almacenada en los archivos de IPCop, pero el servidor DHCP no entregará esta concesión.

Dirección MAC. La dirección MAC de seis octetos/bytes separada por ':' de la máquina a la que se le entregará la concesión fija.

Aviso

El formato de la dirección MAC es `xx:xx:xx:xx:xx:xx`, y no `xx-xx-xx-xx-xx-xx`, como muestran algunas máquinas, p.e. `00:e5:b0:00:02:d2`

Dirección IP. La dirección IP de la concesión fija que el servidor DHCP usará siempre para la dirección MAC asociada. No utilice una dirección del rango de direcciones dinámicas del servidor.

Nombre de host o FQDN (opcional). Puede especificar un nombre de host que siempre se asociará a un dispositivo con una dirección hardware concreta. Un nombre de host especificado así sobreescribe a cualquiera proporcionado por el cliente DHCP de la máquina.

Alternativamente, si no especifica una dirección hardware, la dirección IP se aplicará a cualquier máquina que diga tener ese nombre.

Dirección IP del Enrutador (opcional). Para dar una ruta por defecto a una concesión fija, introduzca la dirección IP aquí.

Servidor DNS (opcional). Para indicar a una concesión fija que utilice un servidor DNS concreto, introduzca su dirección IP aquí.

Identificador (opcional). Si quiere, puede incluir una cadena de texto para identificar al dispositivo que usa la concesión fija.

next-server (opcional). Algunas máquinas de su red pueden ser 'thin clients' que necesitan cargar un archivo de arranque de un servidor de red. Puede especificar la dirección del servidor aquí si es necesario.

Nombre de archivo (opcional). Especifique el archivo de arranque para esta máquina.

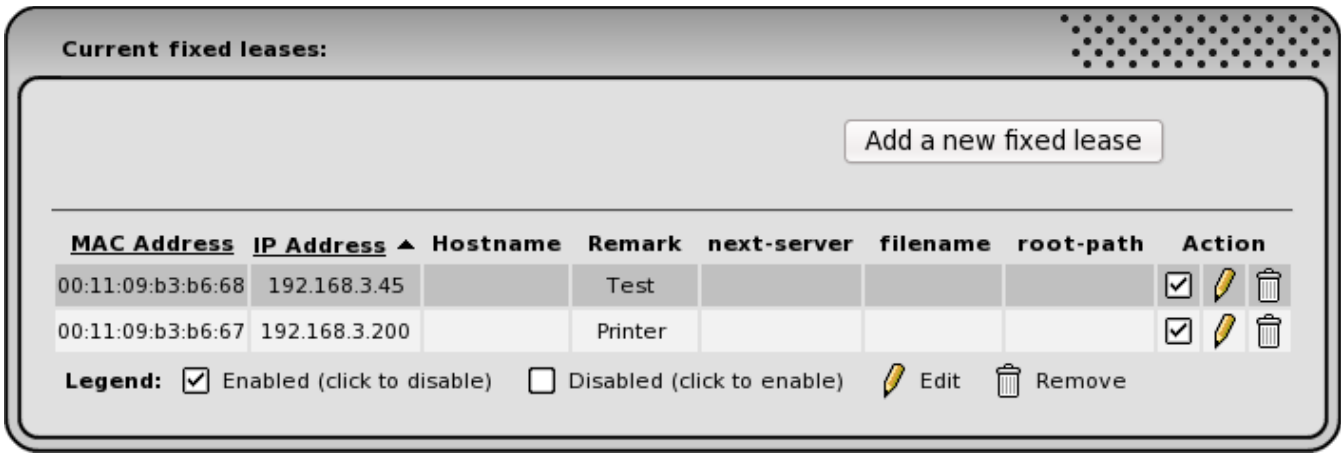
root-path (opcional). Si el archivo de arranque no está en el directorio por defecto, especifique la ruta completa al mismo aquí.

2.5.3.3. Concesiones fijas actuales

Las concesiones fijas actuales se muestran al pie de esta sección, y pueden ser activadas/desactivadas, editadas o borradas.

Puede ordenar la lista de concesiones fijas pinchando en los encabezados subrayados *Dirección MAC* o *Dirección IP*. Otro click en el encabezado invertirá el orden.

Figura 2.29. Lista de concesiones fijas



Para activar o desactivar una entrada, pulse en la casilla de la columna Acción de la concesión que quiera activar o desactivar. El icono cambia a una casilla vacía cuando una concesión fija está desactivada. Pinche en la casilla para activarla de nuevo.

Para editar una concesión, pinche en su icono del *lápiz amarillo*. Los datos de la entrada se mostrarán en el formulario superior. Realice los cambios y pulse el botón Actualizar.

Para borrar una entrada, pinche en su icono de la *papelera*.

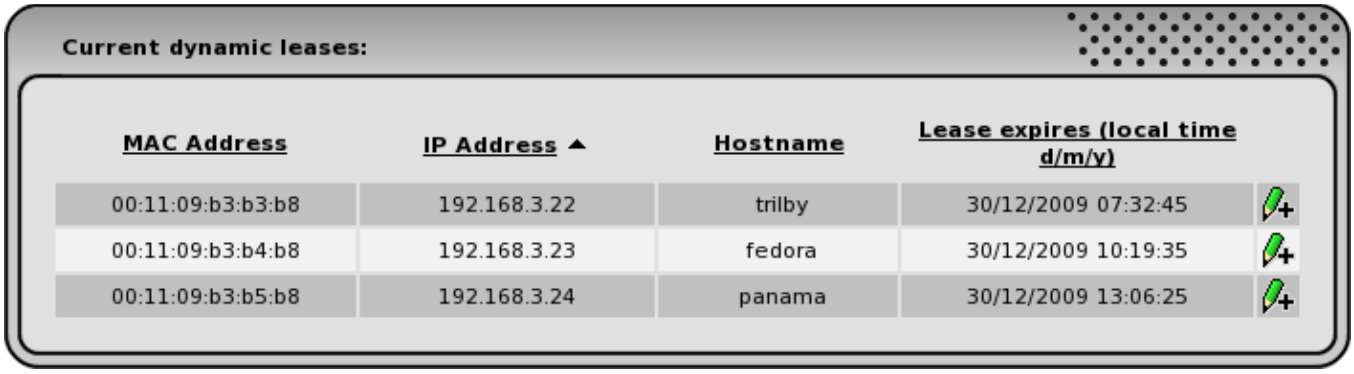
2.5.3.4. Concesiones dinámicas actuales

Si DHCP está activado, esta sección listará las concesiones dinámicas contenidas en el archivo `/var/run/dnsmasq/dnsmasq.leases` Se muestran La dirección IP, dirección MAC, nombre de host (si está disponible) y hora de expiración de la concesión de cada registro, ordenados por dirección IP.

Puede reordenar la lista de concesiones dinámicas pinchando en cualquiera de los cuatro encabezados de columna. Un segundo click invertirá el orden.

Para asignar a uno de los dispositivos en la lista dinámica una concesión fija, pinche en el icono Añadir nueva concesión fija a la derecha de la tabla (el símbolo del *lápiz verde con un '+'*. Esto lo moverá a la sección superior Añadir una nueva concesión fija, y rellenará los campos por usted, dejando elegir una dirección IP.

Figura 2.30. Concesiones dinámicas actuales



2.5.3.5. Opciones DHCP adicionales

Si tiene algún parámetro especial que quiera distribuir a su red mediante el servidor DHCP, añádalo al archivo `/var/ipcop/dhcp/dnsmasq.local` proporcionado para ser utilizado por el usuario. Tras modificar el archivo, reinicie el servidor DHCP mediante la interfaz web o con en comando **restartdhcp** para que los cambios se propaguen a la red.

Vea la sección sobre cómo personalizar dnsmasq.local para ver ejemplos.

2.5.3.6. Mensajes de error

Aparecerá un mensaje de error en lo alto de la página si se encuentra un error en los datos introducidos, tras pulsar el botón Guardar.

2.5.4. Página administrativa de DNS Dinámico

DNS Dinámico (DYNDNS) le permite hacer que su nombre de dominio esté disponible para Internet, incluso aunque no tenga una dirección IP fija.

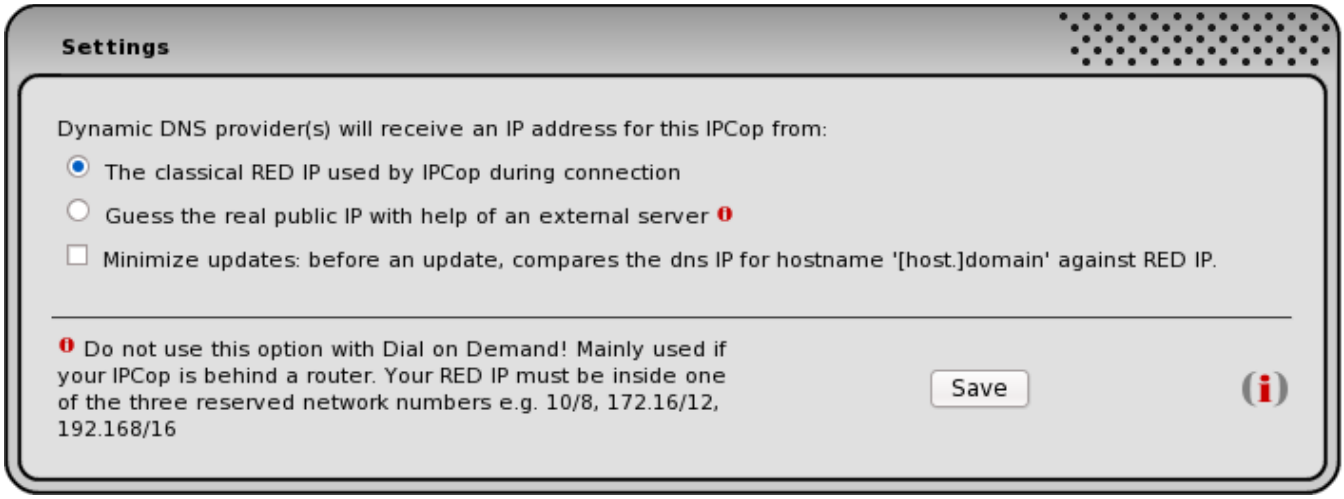
Para usar DYNDNS, primero debe registrar un subdominio con un proveedor DYNDNS. Luego, cada vez que IPCop se conecte a Internet y reciba una dirección IP de su ISP, debe informar al servidor DYNDNS de esa dirección IP. Cuando una máquina cliente quiere conectarse a su dominio, resolverá la dirección yendo al servidor DYNDNS, quien le dará el último valor. Si éste está actualizado, el cliente podrá contactarle (asumiendo que las reglas del cortafuegos permitan esto).

IPCop hace que el proceso de mantener su dirección DYNDNS actualizada sea más fácil, proporcionando actualizaciones automáticas para muchos de los proveedores DYNDNS.

2.5.4.1. Ajustes

La primera sección tiene un par de ajustes generales.

Figura 2.31. Ajustes de DNS Dinámico



El (los) proveedor(es) de DNS Dinámico recibirá(n) una dirección IP de este IPCop desde: Elija 'La IP ROJA clásica usada por IPCop durante la conexión' si si máquina IPCop tiene una IP pública o la IP que usted quiere que sea enviada. Si IPCop falla al detectar su IP pública, elija 'Averiguar la IP pública real con ayuda de un servidor externo'.

Averiguar la IP pública real con ayuda de un servidor externo. Esta opción se usa principalmente si su IPCop está detrás de un enrutador. No use esta opción con Marcado bajo Demanda. Su IP ROJA debe estar dentro de una de estas tres redes privadas p.e. 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16.

Minimizar actualizaciones. Evita muchas actualizaciones al servicio de DNS dinámico comparando la IP registrada con su servicio y la IP que IPCop ha detectado. Debido a que muchos servicios de DNS dinámico pueden denegarle el servicio si actualiza con demasiada frecuencia, se recomienda encarecidamente que seleccione esta opción.

Si su IPCop está conectado 24/7, puede utilizar un evento programado para forzar una actualización y evitar que su cuenta sea declarada 'muerta'. Vea la sección más abajo.

Guardar. Tras realizar cualquier cambio, pulse el botón Guardar para aplicarlo.

2.5.4.2. Añadir un nombre DNS dinámico

La segunda sección le permite Añadir o Editar un registro.

Seleccione un proveedor DYNDNS de la lista desplegable y pulse el botón Añadir. Aparecerá la siguiente pantalla:

Figura 2.32. Añadir un registro de DNS dinámico

Servicio. Debería estar ya registrado en este servicio.

Activado. Si esto no está marcado, IPCop no actualizará la información en el servidor DYNDNS. Guardará la información, de forma que pueda reactivar las actualizaciones DYNDNS sin volver a introducir los datos.

Activar comodines. Activar comodines le permitirá tener todos los subdominios de su nombre DNS dinámico apuntando a la misma IP como su nombre de host (p.e. con esta casilla activada, www.ipcop.dyndns.org apuntará a la misma IP que ipcop.dyndns.org). Esta casilla no funciona con el servicio no-ip.com, ya que sólo permiten activar o desactivar esto directamente en su sitio web.

Algunos de los siguientes campos pueden ser opcionales, dependiendo de su proveedor DYNDNS.

Nombre de host. Introduzca el nombre de host que registró con su proveedor DYNDNS.

Dominio. Introduzca el nombre de dominio que registró con su proveedor DYNDNS.

Nombre de usuario. Introduzca el nombre de usuario con el que se registró en su proveedor DYNDNS.

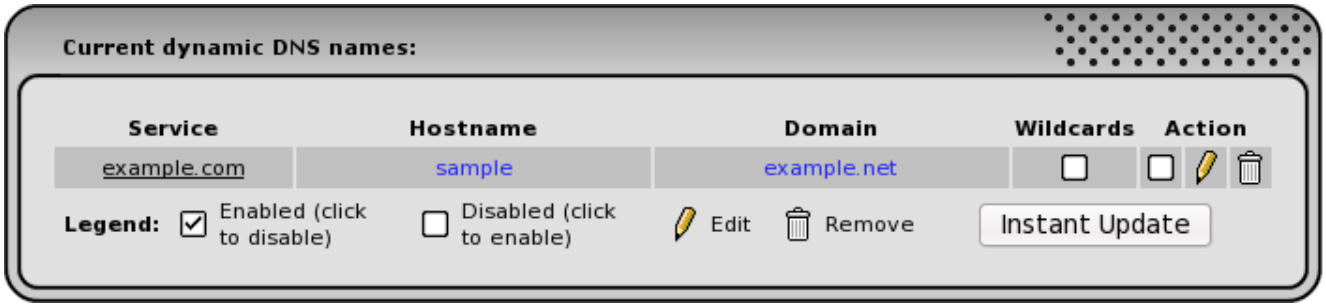
Contraseña. Introduzca la contraseña para su nombre de usuario.

Añadir. Cuando pulse el botón Añadir, los datos se guardan.

2.5.4.3. Nombres DNS dinámicos actuales

Esta sección muestra los registros DNS dinámicos que tiene actualmente configurados.

Figura 2.33. Registros DNS dinámicos actuales



Una entrada en verde indica que la última actualización tuvo éxito, una entrada en azul indica que está inactivo, y una entrada en rojo significa una actualización fallida.

Para editar una entrada, pinche en su icono del *lápiz amarillo*. Los datos de la entrada se mostrarán en el formulario superior. Realice los cambios y pulse el botón Guardar en el formulario.

También puede cambiar las casillas Comodines y Activado directamente en la entrada de la lista de hosts.

2.5.4.4. Forzar una actualización manual

Puede forzar que IPCop refresque la información manualmente pulsando el botón Actualización instantánea, aunque es mejor actualizar solamente cuando la dirección IP ha cambiado realmente, ya que a los proveedores de servicios de DNS dinámico no les gusta manejar actualizaciones que no hacen cambios. Una vez que las entradas de los host se han activado, su IP será automáticamente actualizada cada vez que su IP cambie.

2.5.4.5. Programar una actualización

Para evitar que su cuenta sea declarada 'muerta' debido a falta de actividad, puede forzar a que IPCop refresque la información automáticamente usando el evento programado *Forzar actualización DynDNS* en la página Programador.

Esto es aplicable principalmente a IPCop's que corren sin interrupciones y que no cambian su IP con frecuencia.

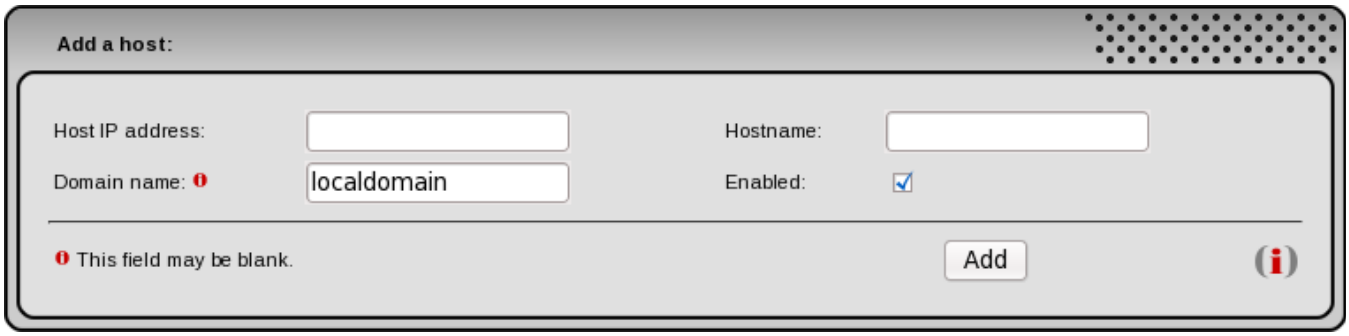
2.5.5. Página administrativa de Edición de Hosts

Además de cachear información DNS de Internet, el proxy DNS de IPCop le permite introducir manualmente hosts cuyas direcciones quiera mantener localmente. Éstas pueden ser direcciones de máquinas locales o máquinas de Internet cuya dirección quiere sobreescribir.

2.5.5.1. Añadir un host

Añada direcciones IP y nombres de host en la primera sección.

Figura 2.34. Añadir un host



Dirección IP del host. Introduzca la dirección IP aquí.

Nombre de host. Introduzca el nombre de host aquí.

Nombre de dominio (opcional). Si el host está en otro dominio, introdúzcalo aquí.

Activado. Marque esta casilla para activar la entrada.

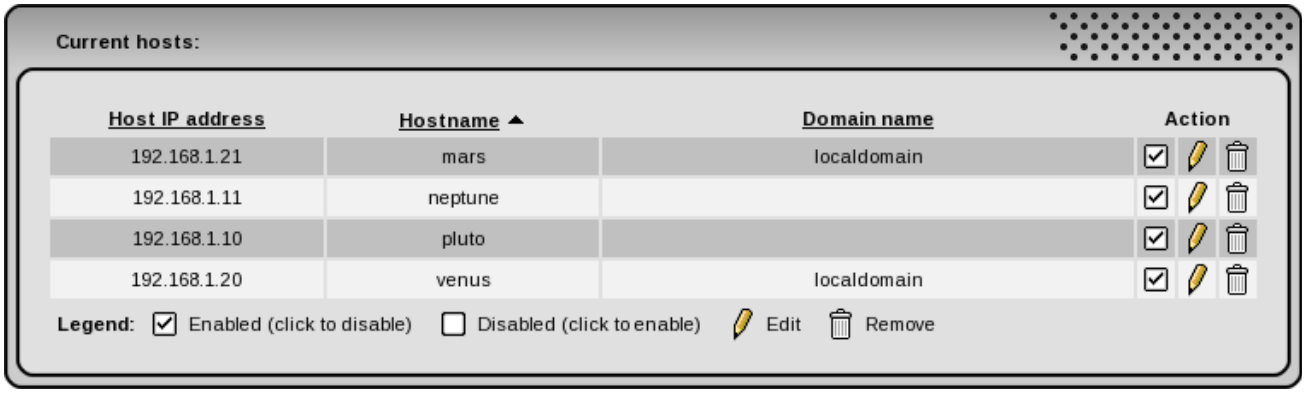
Añadir. Cuando pulse el botón Añadir, los datos se guardan.

2.5.5.2. Hosts actuales

Esta sección muestra las entradas DNS locales que tiene actualmente configuradas.

Puede reordenar la lista pinchando en cualquiera de los tres encabezados de columna. Un segundo click invertirá el orden.

Figura 2.35. Lista de hosts actuales



Para activar o desactivar una entrada, pinche en la casilla de la columna Acción del host que quiere activar o desactivar. El icono cambia a una casilla vacía cuando la entrada está desactivada. Pinche en la casilla para activarla de nuevo.

Para editar una entrada, pinche en el icono del *lápiz amarillo*. Los datos de la entrada se mostrarán en el formulario superior. Realice los cambios y pulse el botón Actualizar en el formulario.

Para borrar una entrada, pinche en su icono de la *papelera*.

2.5.5.3. Añadir una lista de hosts

Digamos que tiene una larga lista de hosts que quiere añadir, como una lista de bloqueo de servidores de'ads', nombres de host y direcciones. En vez de escribirlos uno a uno, puede copiar un archivo de nombres a IPCop, y enlazarlo a **dnsmasq** mediante el archivo `dnsmasq.local`

Vea la sección sobre cómo personalizar dnsmasq.local para ver ejemplos.

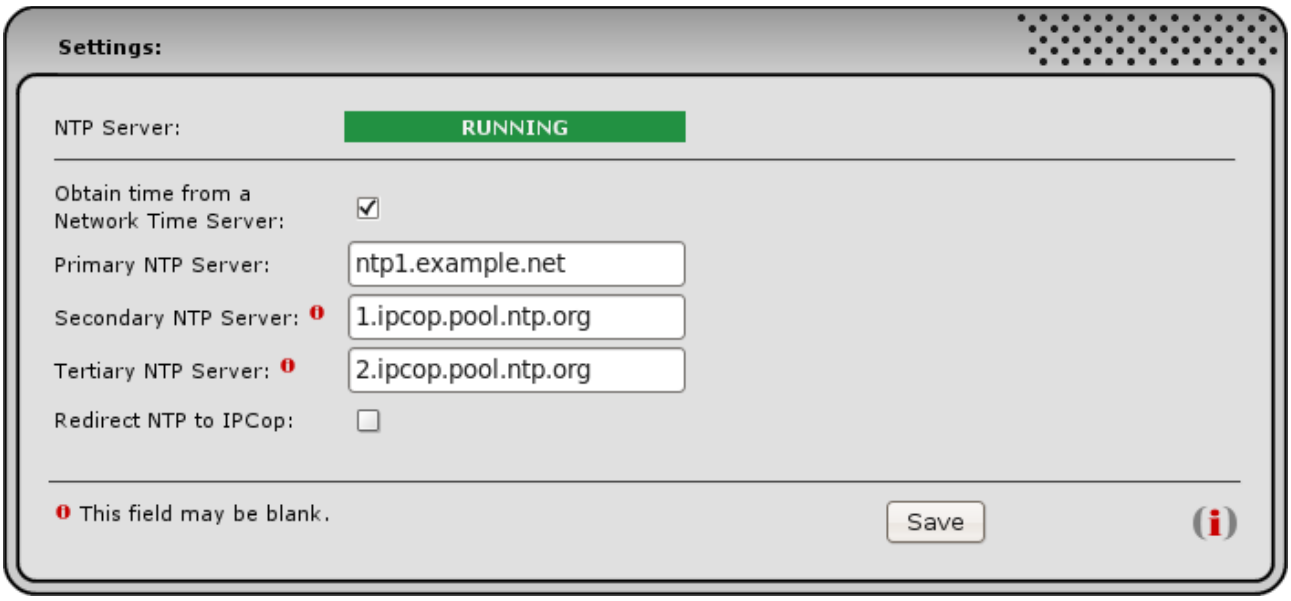
2.5.6. Página administrativa del Servidor horario

IPCop se puede configurar para obtener la hora de servidores horarios precisos en Internet. Además, también puede proporcionar esta hora a otras máquinas de su red.

2.5.6.1. Ajustes

La primera línea en la sección de Ajustes indica si el servidor **ntpd** está parado o corriendo.

Figura 2.36. Ajustes del servidor horario



Para activar el servidor horario, marque la casilla Obtener hora desde un Servidor Horario de Red e introduzca el nombre completo del servidor horario que quiere usar en la casilla Servidor NTP Primario. También puede introducir un Servidor NTP Secundario opcional o Servidor NTP Terciario si lo desea.

Le sugerimos que, para mayor eficiencia, sincronice IPCop con los servidores horarios de su ISP si están disponibles. Si no los tiene, pruebe el proyecto www.pool.ntp.org, que es "un gran cluster virtual de servidores de hora que busca ofrecer un servicio NTP fiable y fácil de usar para millones de clientes sin hacer un uso intensivo de los grandes servidores más populares."

Siga sus instrucciones acerca de cómo usar zonas horarias (por ejemplo `0.us.pool.ntp.org`) en vez de la zona global (`0.pool.ntp.org`), para mejorar aún más la eficiencia.

En Enero de 2008, el conjunto de IPCop empezó a estar disponible. Por favor, utilice `0.ipcop.pool.ntp.org` `1.ipcop.pool.ntp.org` o `2.ipcop.pool.ntp.org` en vez de los anteriores nombres de zona por defecto.

IPCop proveerá un servicio de hora al resto de su red cuando se active el Servidor NTP.

Servidores en la red Naranja

Por favor, tenga en cuenta que IPCop no ofrece ningún servicio a la red Naranja, así que los servidores o dispositivos en la red Naranja no pueden usar IPCop como Servidor horario.

Cualquier servidor o dispositivo en la red Naranja debe usar un Servidor horario de Internet para la sincronización horaria.

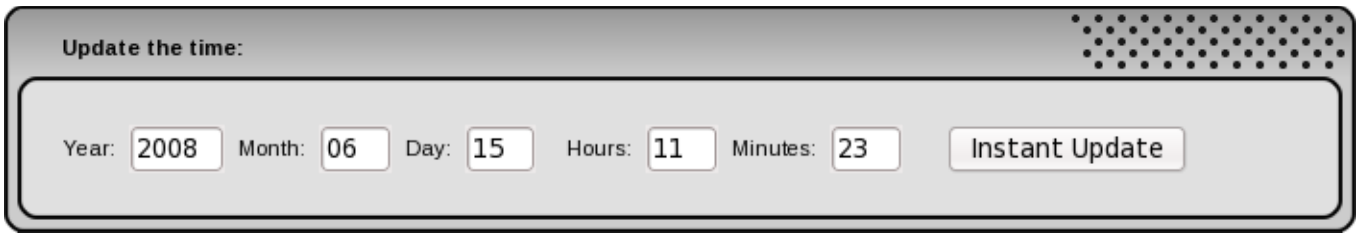
Redirigir NTP a IPCop. Use esta opción para redirigir los equipos configurados para sincronizarse con un servidor NTP fijo en Internet, y que se sincronicen con IPCop en su lugar.

Guardar. Para guardar su configuración, pulse el botón Guardar.

2.5.6.2. Actualizar la hora manualmente

Si no quiere usar un servidor horario de Internet, puede introducir la hora manualmente y pulsar el botón Actualización instantánea.

Figura 2.37. Actualizar la hora



Aviso

Si corrige una gran cantidad de tiempo, y lleva el reloj por detrás de sí mismo, el servidor fcron que corre trabajos cron regularmente puede parecer detenido mientras espera a que la hora le alcance. Esto puede afectar a la generación de gráficos y otras tareas regulares que corren en segundo plano.

Si ocurre esto, intente correr el comando **fcrontab -z** en una terminal para reiniciar el servidor fcron.

2.5.6.3. Cambiar la zona horaria

La zona horaria se definió durante el proceso de instalación.

Para cambiar la zona horaria necesitará volver a correr **setup** desde una terminal.

Acceda como 'root' y ejecute el comando:

```
# setup
```

Seleccione `Zona horaria` del primer menú, y elija una nueva zona horaria de la lista. Pulse el botón Ok cuando haya terminado.

2.5.7. Pagina administrativa de Priorización de Tráfico

La priorización de trafico le permite priorizar el tráfico IP que se mueve a través de su cortafuegos.

IPCop utiliza WonderShaper para hacer esto. WonderShaper fue diseñado para minimizar la latencia de ping, asegurando que el tráfico interactivo como SSH responde, todo ello mientras se descarga o se sube otro tráfico menos importante.

Muchos ISPs venden velocidad como ratios de descarga, no como latencia. Para maximizar las velocidades de descarga, configuran su equipamiento para retener largas colas de su tráfico. Cuando se mezcla tráfico interactivo entre estas largas colas, su latencia se dispara, ya que los paquetes ACK tienen que esperar en línea antes de llegar a usted. IPCop toma cartas en el asunto y prioriza su tráfico de la manera que usted desea. Esto se hace clasificando el tráfico en categorías de Alta, Media y Baja prioridad. El tráfico ping siempre tiene la mayor prioridad, para mostrarle cómo de rápida es su conexión mientras realiza descargas masivas.

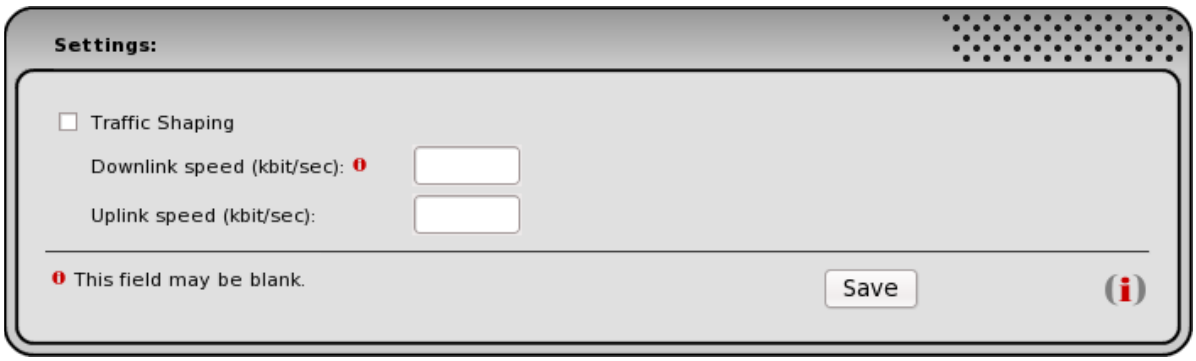
Para usar la Priorización de Tráfico en IPCop:

1. Utilice sitios rápidos conocidos para estimar sus velocidades máximas de descarga y de subida. Introduzca las velocidades en los correspondientes campos Descarga y Subida de la sección Ajustes.

   Puede evitar la priorización en descarga inroduciendo 0 en el campo *Velocidad de bajada*, o dejándolo en blanco.

2. Active la priorización de tráfico seleccionando la casilla, y Guardar sus cambios.

Figura 2.38. Ajustes de Priorización de Tráfico



3. Identifique qué servicios se usan detrás de su cortafuegos.
4. Luego, ordénelos en sus tres grupos de prioridad. Por ejemplo:
    a. Tráfico interactivo como SSH (puerto 22) y VoIP (voice over IP) van en el grupo de prioridad *Alta*.
    b. Su tráfico de navegación y comunicación, como el tráfico web (puerto 80) y el 'streaming' de video/audio van en el grupo de prioridad *Media*.
    c. Ponga el tráfico poco importante, como la compartición de archivos P2P en el grupo de prioridad *Baja*.
5. Cree una lista de servicios y prioridades usando la sección Añadir servicio.

Figura 2.39. Añadir un servicio a la Priorización de Tráfico

Los servicios, más arriba, son sólo ejemplos del potencial de configuración de la Priorización de Tráfico. Dependiendo de su uso, querrá sin duda reordenar sus elecciones de tráfico de alta, media y baja prioridad.

Los paquetes ACK van automáticamente al grupo de prioridad *Alta*. El tráfico que no coincida con ninguno de los servicios definidos va al grupo de prioridad *Media*.

2.6. Menú Cortafuegos

Agrupadas en el menú Cortafuegos, están algunas de las funciones principales de IPCop que controlan cómo pasa el tráfico a través del cortafuegos.

Éstas son:

- Ajustes del Cortafuegos

- Filtro de Direcciones
- Servicios
- Grupos de Servicios
- Direcciones
- Grupos de Direcciones
- Interfaces
- Reglas del Cortafuegos

Las secciones Cambios en la v2.0 y ¿Qué trafico se permite entre interfaces? contienen información adicional sobre el cortafuegos.

2.6.1. Cambios en la v2.0

Acceso a IPCop. IPCop ya no acepta todos los paquetes enviados desde interfaces internas, sino únicamente paquetes para servicios que IPCop conoce (DHCP, DNS, NTP, Proxy, IPsec, OpenVPN).

Reenvío de puertos. El reenvío de puertos ahora se controla en la página Reglas del Cortafuegos.

Acceso externo. El acceso externo se controla también en la página Reglas del Cortafuegos.

DMZ Pinholes. Se pueden crear entre redes en la página Reglas del Cortafuegos.

Acceso Azul. El acceso a la red Azul aún se puede controlar en la página Filtro de Direcciones. Además, ahora es posible desactivar los controles completamente editando la política de la interfaz en la página Ajustes del Cortafuegos.

Opciones del Cortafuegos. La posibilidad de desactivar las respuestas a ping desde ciertas interfaces ya no está disponible. Si quiere desactivar la respuesta a ping, necesita crear una 'Regla de Cortafuegos' con la acción 'Drop' para ping.

2.6.2. ¿Qué tráfico se permite entre interfaces?

El modelo de seguridad de IPCop es que la red VERDE es completamente confiable y cualquier petición desde esta red, ya sea iniciada por un usuario o por una máquina infectada por un virus, troyano u otro “malware” es legítima y permitida para IPCop.

Una nueva característica de IPCop, permite asignar políticas para cada interfaz de red. Esto hace posible permitir sólo un tráfico específico a ROJA y a IPCop.

El orden de confianza de las redes, de menor a mayor es:

ROJA→NARANJA→AZUL→VERDE

Las siguientes tablas listan el comportamiento entre interfaces y hacia IPCop dependiendo de la política configurada y el tipo de regla requerido para permitir (o denegar) el tráfico.

Tabla 2.1. VERDE

Origen	Política	Destino	Tipo de regla	
VERDE	Abierta	**IPCop**	Abierto para Servicios conocidos	Acceso a IPCop
VERDE	Abierta	**ROJA**	Abierto	Saliente
VERDE	Abierta	**NARANJA**	Abierto	Interno
VERDE	Abierta	**AZUL**	Abierto	Interno
VERDE	Semi-Abierta	**IPCop**	Abierto para Servicios conocidos	Acceso a IPCop
VERDE	Semi-Abierta	**ROJA**	Cerrado	Saliente
VERDE	Semi-Abierta	**NARANJA**	Cerrado	Interno
VERDE	Semi-Abierta	**AZUL**	Cerrado	Interno
VERDE	Cerrada	**IPCop**	Cerrado	Acceso a IPCop
VERDE	Cerrada	**ROJA**	Cerrado	Saliente
VERDE	Cerrada	**NARANJA**	Cerrado	Interno
VERDE	Cerrada	**AZUL**	Cerrado	Interno

Las interfaces IPsec y OpenVPN son iguales a VERDE y su comportamiento es el mismo.

Tabla 2.2. ROJA

Origen	Política	Destino		Tipo de regla
ROJA	Cerrada	**IPCop**	Cerrado	Acceso Externo
ROJA	Cerrada	**VERDE**	Cerrado	Reenvío de puertos
ROJA	Cerrada	**NARANJA**	Cerrado	Reenvío de puertos
ROJA	Cerrada	**AZUL**	Cerrado	Reenvío de puertos

Tabla 2.3. AZUL

Origen	Política	Destino		Tipo de regla
AZUL	Abierta	**VERDE**	Cerrado	Interno
AZUL	Abierta	**IPCop**	Abierto para Servicios conocidos	Acceso a IPCop
AZUL	Abierta	**ROJA**	Abierto	Saliente
AZUL	Abierta	**NARANJA**	Abierto	Interno
AZUL	Semi-Abierto	**VERDE**	Cerrado	Interno
AZUL	Semi-Abierto	**IPCop**	Abierto para Servicios conocidos	Acceso a IPCop
AZUL	Semi-Abierta	**ROJA**	Cerrado	Saliente
AZUL	Semi-Abierta	**NARANJA**	Cerrado	Interno
AZUL	Cerrada	**VERDE**	Cerrado	Interno
AZUL	Cerrada	**IPCop**	Cerrado	Acceso a IPCop
AZUL	Cerrada	**ROJA**	Cerrado	Saliente
AZUL	Cerrada	**NARANJA**	Cerrado	Interno

Tabla 2.4. NARANJA

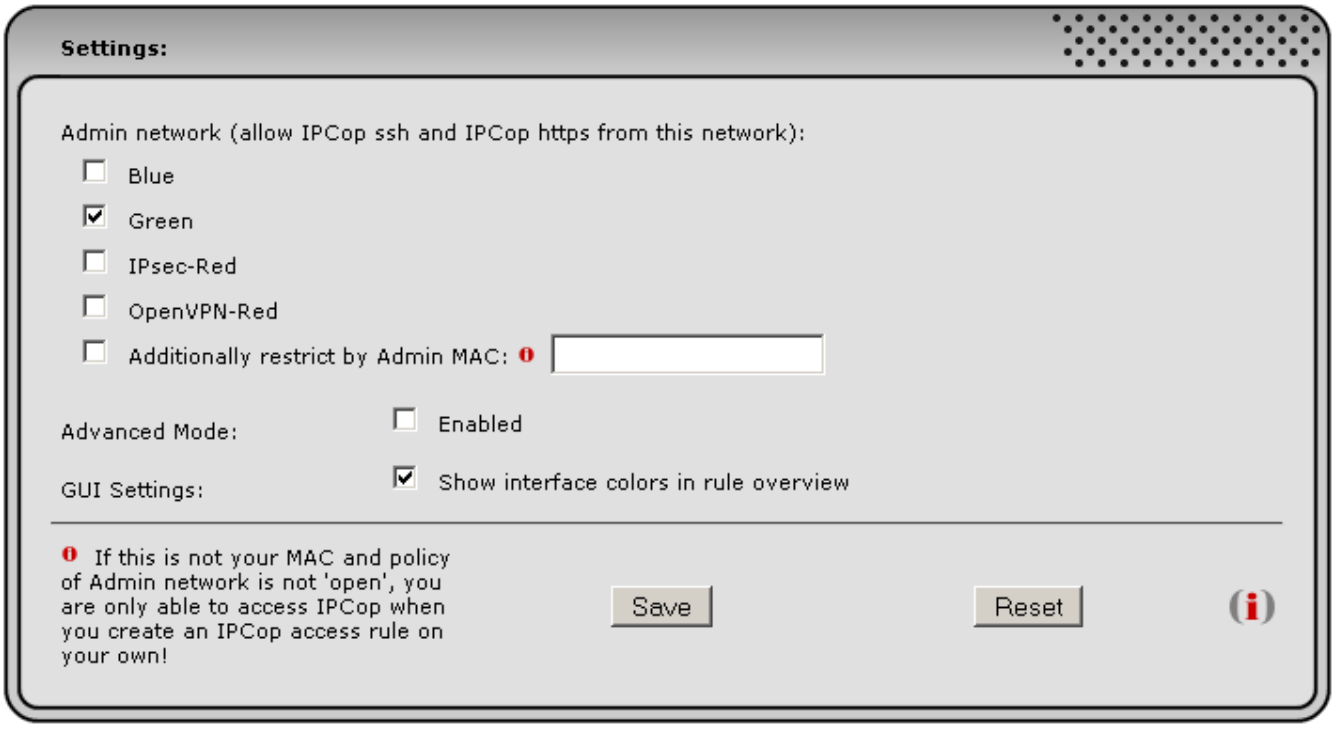
Origen	Política	Destino		Tipo de regla
NARANJA	Abierta	**VERDE**	Cerrado	Interno
NARANJA	Abierta	**IPCop**	Cerrado	-
NARANJA	Abierta	**ROJA**	Abierto	Saliente
NARANJA	Abierta	**AZUL**	Cerrado	Interno
NARANJA	Cerrada	**VERDE**	Cerrado	Interno
NARANJA	Cerrada	**IPCop**	Cerrado	-
NARANJA	Cerrada	**ROJA**	Cerrado	Saliente
NARANJA	Cerrada	**AZUL**	Cerrado	Interno

2.6.3. Página de Ajustes Administrativos del Cortafuegos

2.6.3.1. Ajustes

La primera sección le permite controlar el acceso administrativo (mediante https y ssh) a redes específicas (Verde, Azul, OpenVPN, IPsec) según la disponibilidad.

Figura 2.40. Ajustes del Cortafuegos



Red de Administración. Marque las casillas junto a cada interfaz de red que quiera abrir para acceso administrativo.

Si quiere acceso ssh, no olvide activarlo en la página Acceso SSH.

Si se introduce una dirección MAC, se combina, con lo que si activa Verde y Azul, *e* introduce una dirección MAC, sólo esta máquina tendrá acceso administrativo tanto desde Verde como desde Azul.

Siempre se pueden crear reglas adicionales para permitir tráfico creando reglas de cortafuegos.

Modo Avanzado. Marque esta casilla para añadir varias opciones, usadas con menor frecuencia, cuando cree reglas de cortafuegos.

- Opción para limitar el registro.
- Opción para añadir un lapso de tiempo durante el cual una regla estará activa (supongamos que desea permitir la navegación web para sus niños solamente entre las 19:00 y las 21:00; así es como se hace).
- Añadir interfaces personalizadas.
- Crear reglas para interfaces personalizadas.
- Añadir un puerto de origen a las reglas.
- Añadir la posibilidad de invertir Origen, Destino, Puerto de Origen y Servicio de Destino.

Ajustes de la GUI. Mostrar color de las interfaces en la vista de reglas.

Marque esta casilla para resaltar los colores de las interfaces en la vista de reglas actuales en la página Reglas del Cortafuegos.

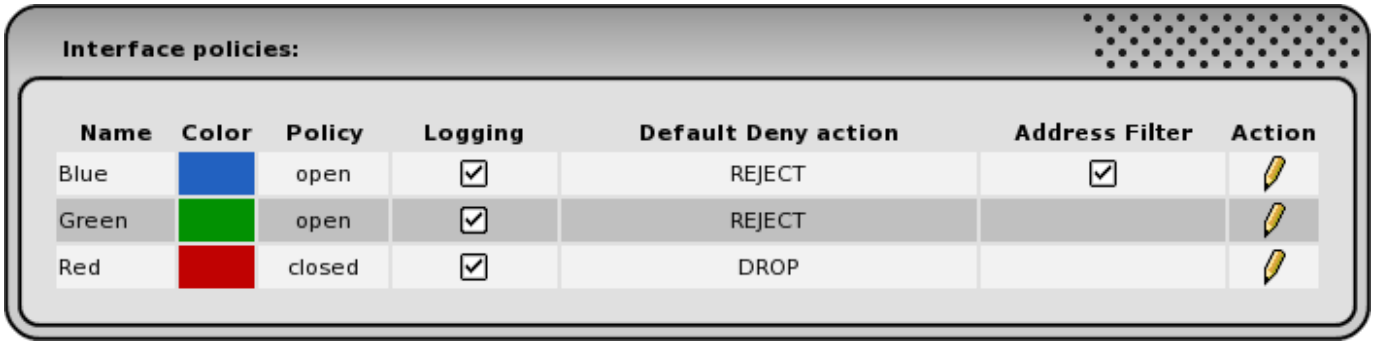
Guardar. Pulse el botón Guardar para guardar sus ajustes.

Revertir. Pulse el botón Revertir para volver a los ajustes por defecto.

2.6.3.2. Políticas de Interfaz

La segunda sección muestra las interfaces activas en el momento y sus ajustes de registro y política.

Figura 2.41. Políticas de Interfaz



Para cada interfaz hay varios ajustes, el primero (y más importante) es la **política**.

Hay tres políticas:

Abierta. Esto abre una interfaz a interfaces de igual y menor seguridad. Esto también abre el acceso a los servicios de IPCop.

Semi-Abierta. Esto abre el acceso a los servicios de IPCop.

Cerrada. Cierra completamente una interfaz. Si se necesita acceso desde una interfaz "cerrada" se debe crear una regla específica.

Nota

No hay política semi-abierta para Naranja.

Solamente hay política cerrada para Roja.

Registro. Con un simple click se puede deshabilitar el registro de una interfaz. (Esto evita llenar su disco duro con intentos de 'ataques' bloqueados desde Internet).

Marque la casilla de nuevo para activar el registro.

Acción de negación por defecto. Rechazar o descartar.

La recomendación es emplear Descartar para Roja, y Rechazar para el resto de interfaces.

Descartar, descarta un paquete silenciosamente. Rechazar, rehusa un paquete y envía un mensaje ICMP 'puerto no alcanzable' de vuelta al origen.

Probablemente no quiera usar Rechazar para paquetes que vengan desde Internet, ya que potencialmente puede llevar a un DoS (negación de servicio).

Para interfaces internas es una buena idea utilizar Rechazar. El cliente recibe un mensaje de error inmediatamente y no tiene que esperar a un 'timeout'.

Filtro de Direcciones. Si el control por Filtro de Direcciones está activado, sólo aquellos clientes que estén en la lista de Filtro de direcciones tendrán acceso, dependiendo de la política.

Los clientes que no estén en la lista de Filtro de Direcciones sólo pueden usar DHCP y abrir túneles IPsec y/o OpenVPN.

Si el control por Filtro de Direcciones *no* está activado, todos los clientes tendrán acceso, dependiendo de la política.

Esto sólo se aplica si tiene una interfaz de red Azul instalada.

Acción. Pinche en el icono del *lápiz amarillo* para editar una política.

2.6.3.3. Ajustes por defecto

Verde es la única interfaz de red para Administración por defecto.

La interfaz Roja tiene 'cerrada' como política por defecto. Todas las demás interfaces tienen 'abierta'.

La interfaz Roja tiene 'Descartar' como Acción de negación. Todas las demás interfaces tienen 'Rechazar'.

El registro está activo en todas las interfaces.

El control por Filtro de Direcciones está activado.

2.6.4. Página Administrativa de Filtro de Direcciones

Esta sección le permite configurar un punto de acceso inalámbrico a la red Azul conectada a IPCop. Esto es 100% opcional, así que puede ignorar esta sección si no desea emplear esta característica.

Nota

Esta página *sólo* estará visible si tiene una interfaz de red Azul instalada y configurada.

2.6.4.1. Ajustes

Para configurar el Filtro de Direcciones haga lo siguiente:

1. Utilice una tarjeta de red soportada para configurar la interfaz Azul.
2. Conecte un punto de acceso a esa tarjeta de red. (Utilice un puerto LAN del punto de acceso en caso de que haya varios tipos).
3. Puede emplear DHCP para servir direcciones dinámicas o fijas en Azul, aunque es preferible usar fijas por seguridad al usar direcciones MAC. Consulte la sección Servidor DHCP para más información sobre cómo configurar concesiones fijas.

Si sólo necesita proporcionar acceso a tráfico http desde la red Azul a Internet (red Roja), simplemente añada la dirección IP o la dirección MAC del enrutador inalámbrico, o de cada uno de los dispositivos inalámbricos conectados en caso de utilizar un punto de acceso, mediante la página mostrada más abajo. Deberá introducir al menos una dirección MAC *o* una dirección IP por dispositivo. Opcionalmente, puede introducir ambas (dirección IP y MAC) para un dispositivo.

Un punto de acceso se comporta como un hub ethernet, y IPCop sirve concesiones DHCP a través de él a los dispositivos inalámbricos. Un enrutador inalámbrico hace NAT, sirve DHCP en su propia subred, y tiene sus propios controles de acceso.

Nota

Su punto de acceso debe soportar el paso DHCP si quiere que IPCop sirva concesiones a través de él a la red inalámbrica. No todos los dispositivos soportan esta característica en “modo” punto de acceso (Netgear WG614, por ejemplo).

Podrá ver la interfaz web de IPCop desde un ordenador en la red Azul, pero no podrá conectarse a la red Verde sin algo más de trabajo.

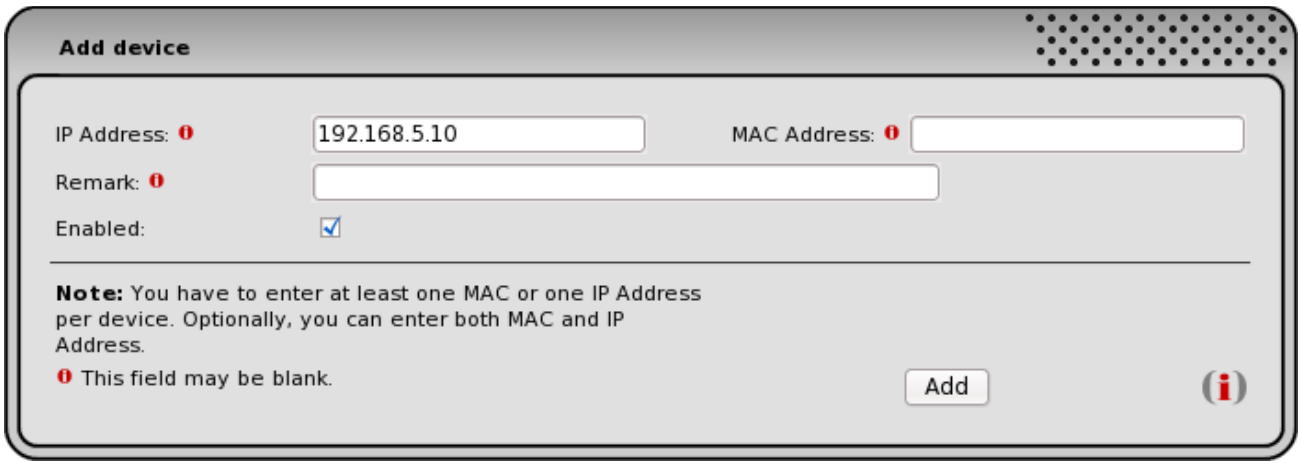
Para conectarse a la red Verde desde la red Azul, debe:

1. Usar la página Reglas de Cortafuegos y crear reglas de Tráfico Interno para abrir pasos a través de la red Azul para sus servicios, o:
2. Configurar una VPN para proporcionar acceso a los "road-warriors" en Azul.

2.6.4.2. Añadiendo un dispositivo

En la sección Añadir dispositivo introduzca la dirección IP o la dirección MAC de un punto de acceso inalámbrico, o cualquier dispositivo en la red Azul que quiera que se conecte a Internet a través de IPCop.

Figura 2.42. Añadir dispositivo



Dirección IP (opcional). Debe introducir al menos una dirección IP *o* MAC por dispositivo, o ambas.

Si usa DHCP en la red Azul, y quiere permitir que cualquier dispositivo se conecte y acceda a la red Roja, debe añadir una entrada para cada dirección IP del rango DHCP a esta lista. Deje el campo Dirección MAC vacío cuando añada cada dirección IP.

Dirección MAC (opcional). Por el contrario, si quiere restringir el acceso a dispositivos conocidos, añada la dirección MAC de cada dispositivo y deje el campo Dirección IP vacío. Esto permitirá a los dispositivos listados conectarse, independientemente de la concesión DHCP que reciban.

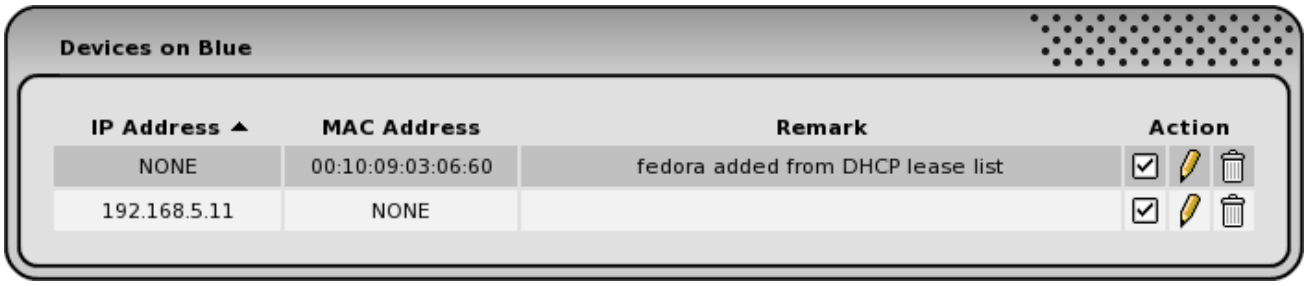
Nombre (opcional). Si quiere, puede incluir una cadena de texto para describir o identificar el dispositivo.

Añadir. Una vez que haya introducido toda la información, pulse el botón Añadir. Esto moverá la entrada a la sección siguiente, y la listará como activada.

2.6.4.3. Dispositivos actuales

La sección Dispositivos en Azul lista las entradas actuales.

Figura 2.43. Dispositivos en Azul

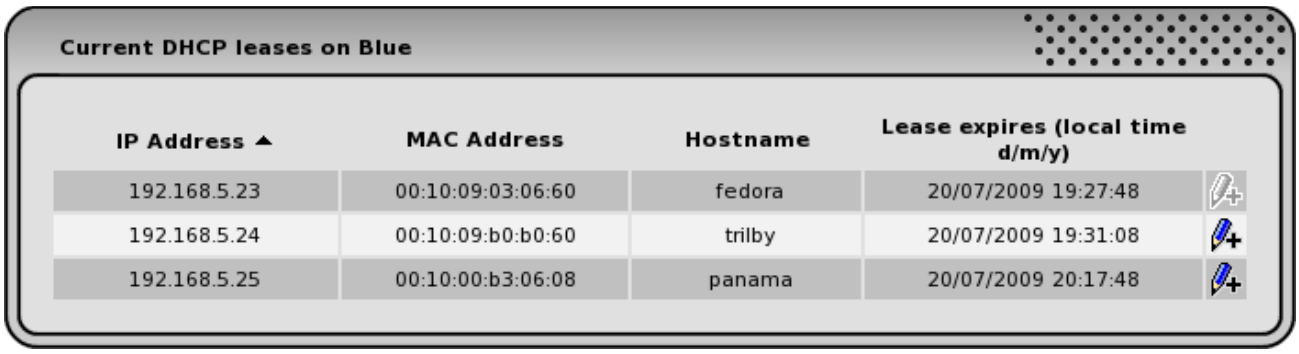


Para eliminar una entrada, pulse el icono de la *papelera*. Para editarla, pulse el icono del *lápiz amarillo*.

Para activar o desactivar un dispositivo, pulse en la casilla de la columna Acción del dispositivo que quiere activar o desactivar. El icono cambia a una casilla vacía cuando un dispositivo está desactivado. Pulse la casilla para activarlo de nuevo.

Si el servidor DHCP está activado para la red Azul, se mostrará la sección Concesiones actuales en Azul.

Figura 2.44. Concesiones actuales en Azul



hay una forma rápida de añadir máquinas a la lista de dispositivos. Sólo tiene que pulsar en el icono del *lápiz azul* para que el dispositivo se añada a la lista de dispositivos activos.

Entonces puede editar la entrada, si es necesario, pulsando el icono del *lápiz amarillo*, como antes.

2.6.4.4. Punto de acceso abierto

Si no necesita o no quiere controlar quién se conecta a Internet (red Roja) a través del punto de acceso Azul, de forma que cualquier dispositivo inalámbrico pueda unirse a la red Azul:

1. Active DHCP en Azul.
2. Desactive el control por Filtro de Direcciones en la sección Política de Interfaz del cortafuegos.

No necesita añadir dispositivos o direcciones individuales cuando el control por Filtro de Direcciones está desactivado.

2.6.5. Página administrativa de Servicios

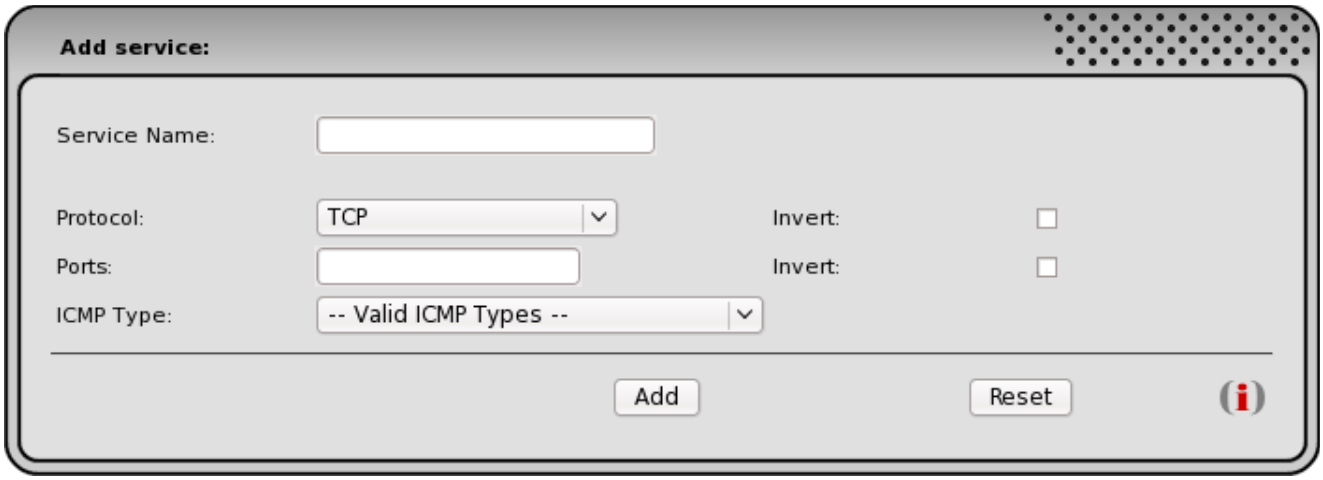
El cortafuegos IPCop está configurado mediante el uso de Servicios y/o Grupos de Servicios.

Si quiere crear una regla para un Servicio que no esté presente en la lista de Servicios por defecto, deberá añadirlo antes.

2.6.5.1. Añadiendo un servicio

En la primera sección proporciona un nombre descriptivo al Servicio personalizado, elige el protocolo y el puerto (sólo TCP y UDP).

Figura 2.45. Añadir un servicio



Nota

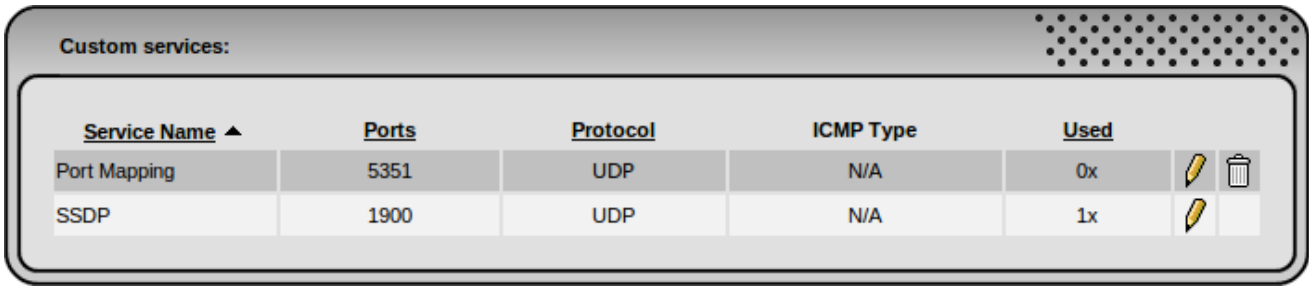
¡Use la opción Invertir con mucho cuidado, ya que puede crear agujeros mucho más grandes en su cortafuegos IPCop de lo que podría esperar!

2.6.5.2. Servicios personalizados

La segunda sección lista los servicios personalizados que ha añadido.

Puede reordenar la pantalla de servicios pinchando en cada uno de los cuatro encabezados de columna subrayados. Otra pulsación más invertirá el orden.

Figura 2.46. Servicios personalizados



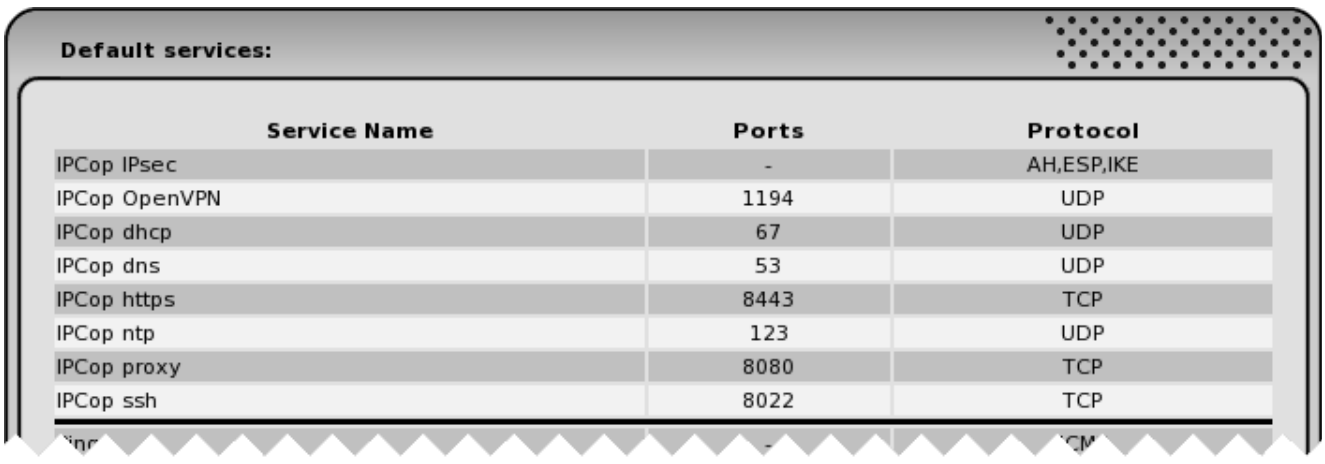
Para editar un servicio, pulse en su icono de *lápiz amarillo*. La entrada se mostrará en el formulario superior. Realice los cambios y pulse el botón Actualizar.

Para borrar un servicio, pulse en su icono de la *papelera*. Sólo podrá borrar un servicio si no está en uso.

2.6.5.3. Servicios por defecto

La tercera sección lista los servicios por defecto.

Figura 2.47. Servicios por defecto



2.6.6. Página administrativa de Grupos de servicios

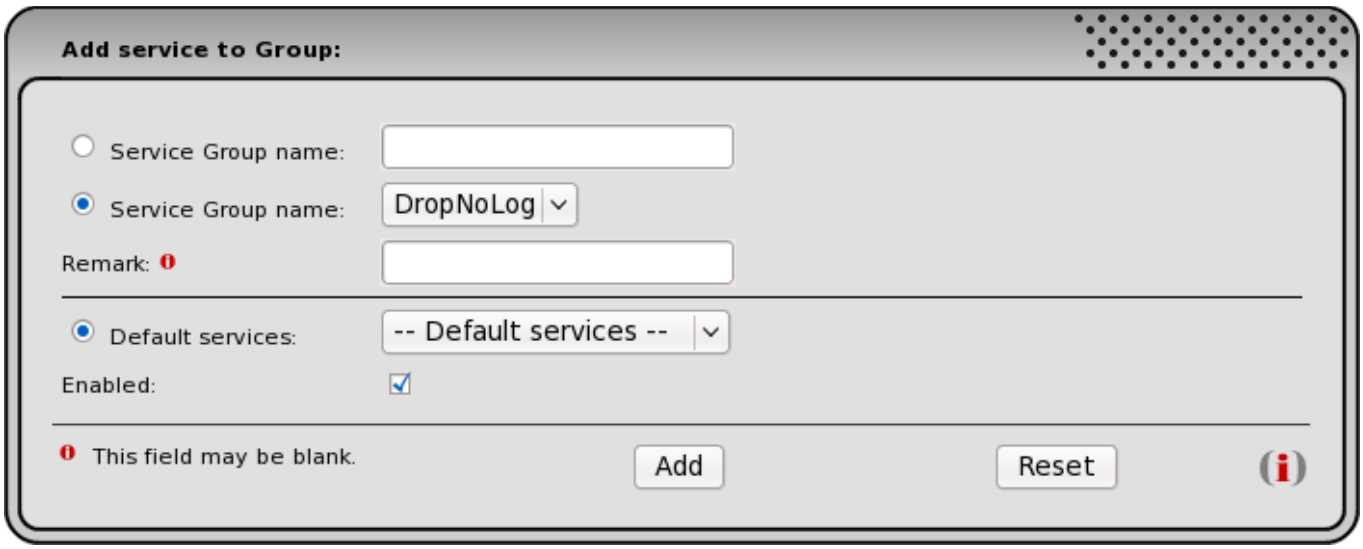
El cortafuegos IPCop está configurado mediante el uso de Servicios y/o Grupos de Servicios.

Los Grupos de servicios le permiten combinar varios Servicios en un Grupo. Luego podrá crear regla(s) que combinen todos los Servicios en un solo paso.

2.6.6.1. Añadir servicio a Grupo

En la primera sección, cree un Grupo de Servicios con un nombre y añada Servicios por defecto o Servicios personalizados si han sido creados. Una vez que se ha creado un Grupo, puede ser seleccionado y añadido desde el menú desplegable.

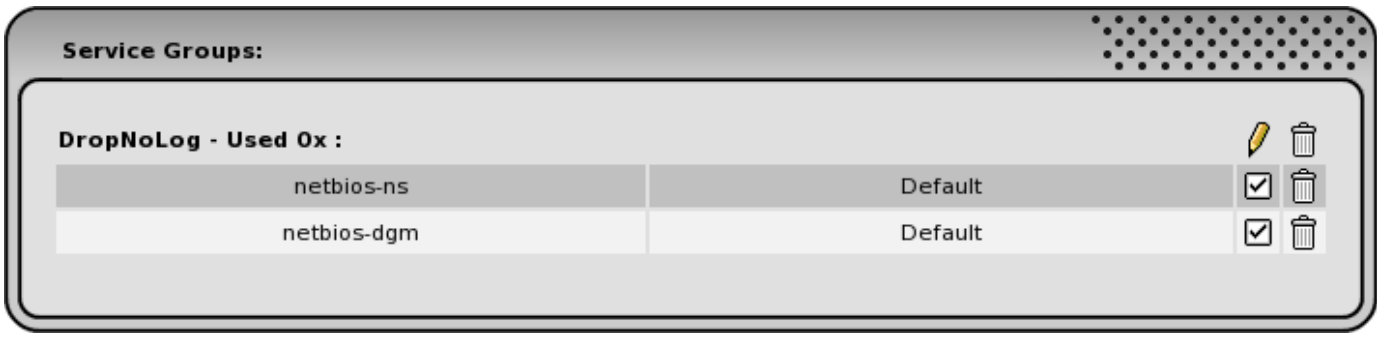
Figura 2.48. Añadir servicio a Grupo



2.6.6.2. Grupos de Servicios

La segunda sección lista los Grupos de Servicio que ha creado.

Figura 2.49. Grupos de servicios



En el ejemplo de arriba, se ha creado un Grupo 'DropNoLog' que incluye algunos Servicios que conocemos y que no queremos que nos llenen el registro del cortafuegos.

Descartar y no registrar netbios-dgm (tcp+udp/138) y netbios-ns (tcp+udp/137) evita que el registro se llene con broadcasts de Netbios.

2.6.7. Página adminstrativa de Ajustes de Direcciones

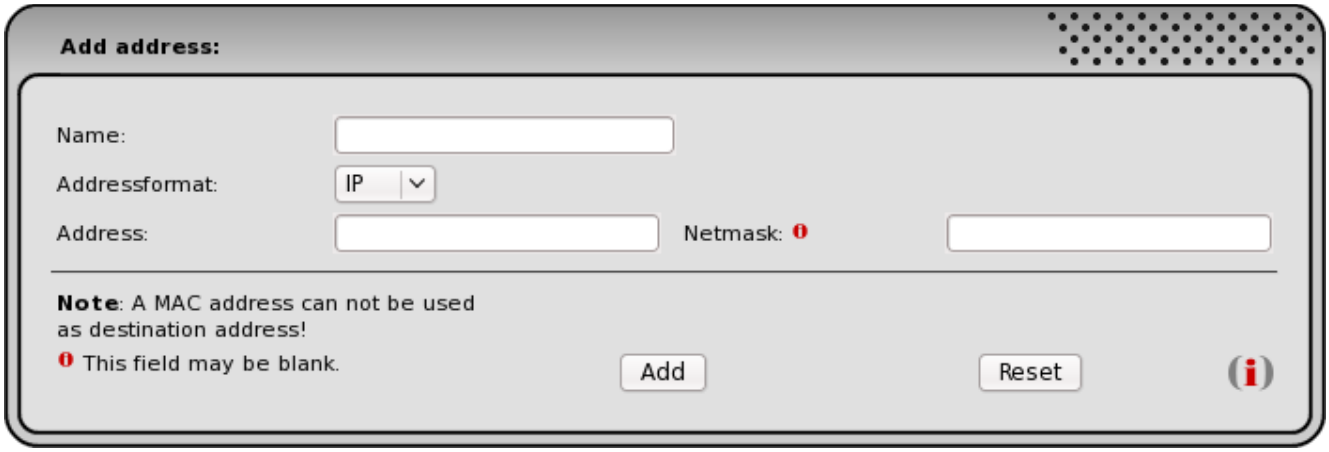
Puede asignar nombres a direcciones IP, redes IP y direcciones MAC.

La ventaja de usar nombres es que cuando tiene que cambiar la dirección IP de un servidor interno o cambiar una tarjeta de red (con una MAC diferente), sólo hay un lugar que requiere modificaciones, y no tiene que cambiar múltiples reglas salientes, pinholes y redirecciones de puertos.

2.6.7.1. Añadir dirección

En la primera sección proporciona un nombre para una dirección o red.

Figura 2.50. Añadir dirección



Nombre. Introduzca un nombre.

Formato de dirección. Seleccione IP o MAC del menú desplegable.

Dirección. Introduzca la dirección.

Nota

Las direcciones MAC sólo pueden usarse en reglas como origen, no como destino.

Máscara de red (opcional). Si el campo máscara de red se deja vacío cuando se define una dirección IP, se usará la máscara 255.255.255.255.

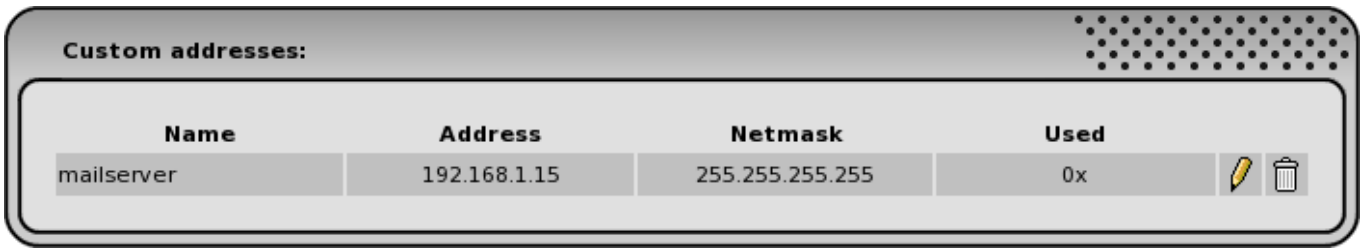
Añadir. Una vez que haya introducido toda la información, pulse el botón Añadir. Esto moverá la entrada a la siguiente sección.

Reiniciar. Pulse el botón Reiniciar para revertir los ajustes a los por defecto.

2.6.7.2. Direcciones personalizadas

La segunda sección contiene una lista de sus direcciones personalizadas.

Figura 2.51. Lista de direcciones personalizadas

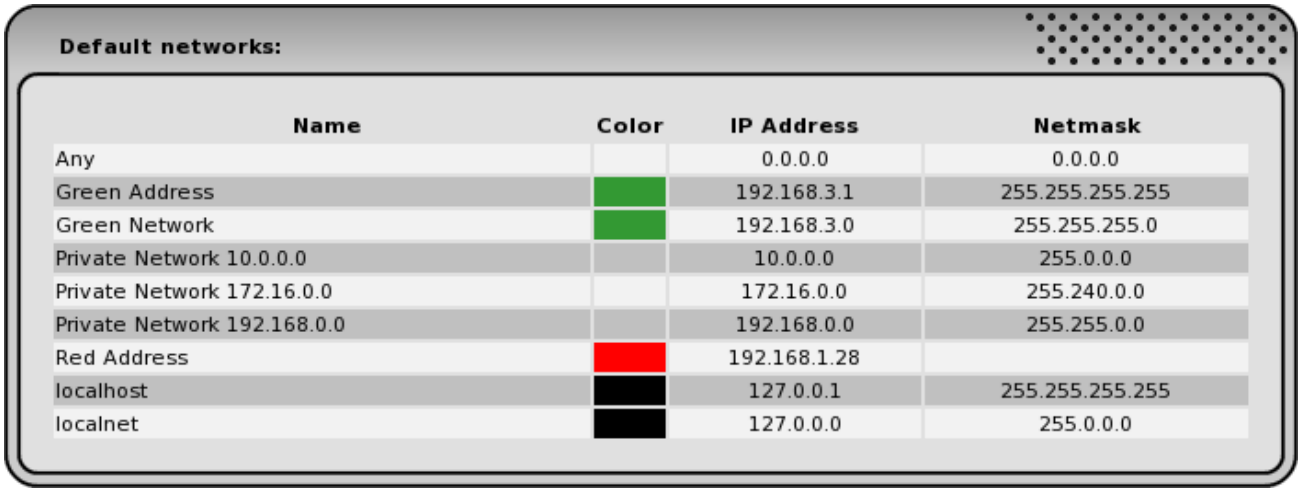


Para borrar una entrada, pulse el icono de la *papelera*. Para editarla, pulse en el icono del *lápiz amarillo*.

2.6.7.3. Redes por defecto

La tercera sección contiene información sobre las redes.

Figura 2.52. Lista de redes por defecto



2.6.8. Página administrativa de Grupos de direcciones

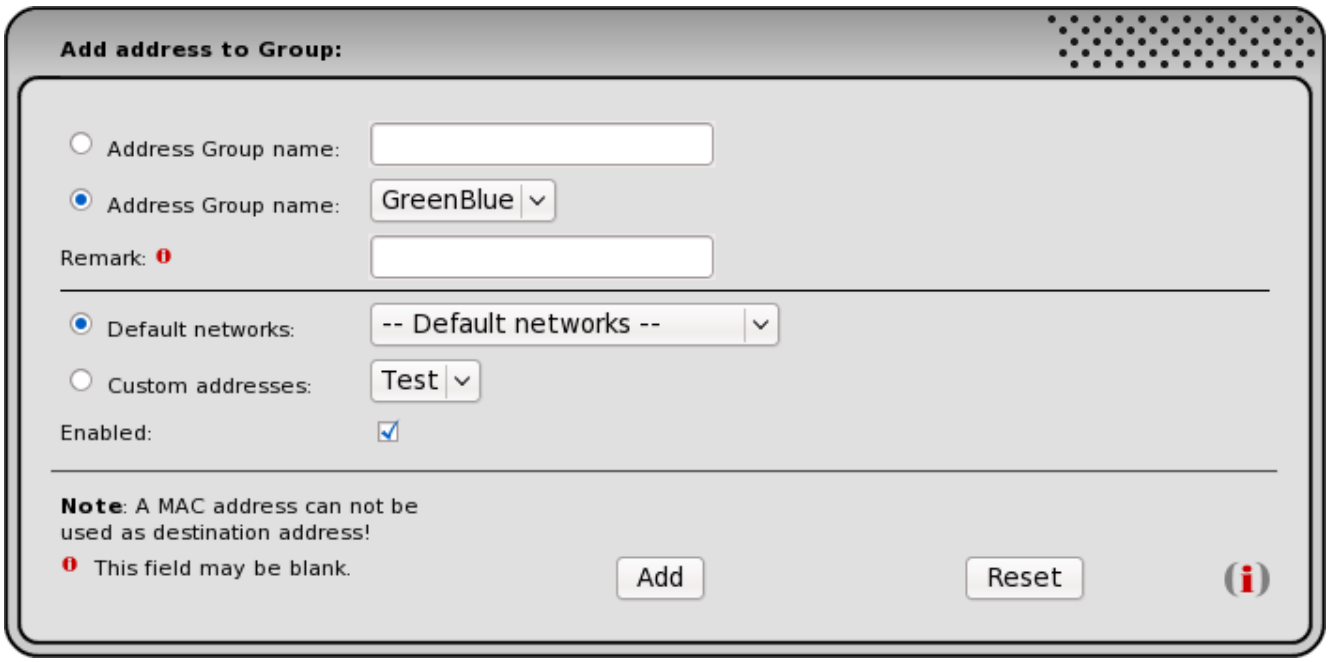
Las direcciones por defecto (por ejemplo, red Verde, red Azul, etc.) y los nombres de direcciones se pueden combinar en grupos.

En un grupo de direcciones puede combinar la red Verde y Azul y luego permitir un servicio concreto para este grupo con una regla.

2.6.8.1. Añadir dirección a grupo

En la primera sección cree un Grupo de direcciones con un nombre y añada redes por defecto o direcciones personalizadas si han sido creadas. Una vez que se crea un Grupo, puede ser seleccionado y añadido desde el menú desplegable.

Figura 2.53. Añadir dirección a grupo



También puede combinar Nombres de dirección en un grupo. Por ejemplo, si tiene varios ordenadores en Azul, pero sólo quiere crear un pinhole para dos portátiles concretos.

Nota

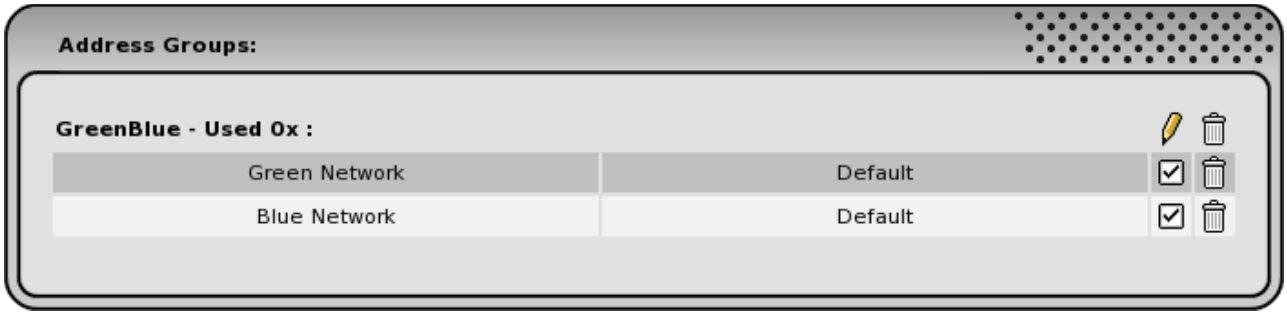
Los grupos no pueden ser utilizados como destino de un reenvío de puertos.

2.6.8.2. Grupos de direcciones

La segunda sección lista los grupos de direcciones que ha creado.

En el ejemplo inferior se han combinado las redes Verde y Azul en un grupo llamado VerdeAzul.

Figura 2.54. Lista de Grupos de Direcciones



Para borrar una entrada, pulse el icono de la *papelera*. Para editarla, pulse en el icono del *lápiz amarillo*.

Para activar o desactivar una entrada, pulse la casilla de la dirección que desee activar o desactivar. El icono cambia a una casilla vacía cuando una dirección está desactivada. Pulse en la casilla para activarla de nuevo.

2.6.9. Página administrativa de Interfaces

Hay casos especiales donde hay presentes otras interfaces, además de las estándar Verde, Azul, Naranja y Roja. Tras asignar un nombre a dichas interfaces, es posible crear reglas de cortafuegos para ellas.

Nota

Interfaces Personalizadas sólo está disponible si está activado el 'Modo Avanzado' en la página Ajustes del cortafuegos.

2.6.9.1. Añadir interfaz

En la primera sección dé un nombre a la Interfaz.

Figura 2.55. Añadir interfaz

Nombre. El nombre para su interfaz. No utilice comas.

Interfaz. En este campo sólo pueden usarse letras minúsculas y mayñusculas, números y los caracteres especiales - _ . :.

Añadir. Una vez que haya introducido toda la información, pulse el botón Añadir. Esto moverá la entrada a la siguiente sección.

Reiniciar. Pulse el botón Reiniciar para revertir los ajustes a los por defecto.

Nota

Aún necesitará asignar drivers y direcciones IP manualmente.

2.6.9.2. Interfaces personalizadas

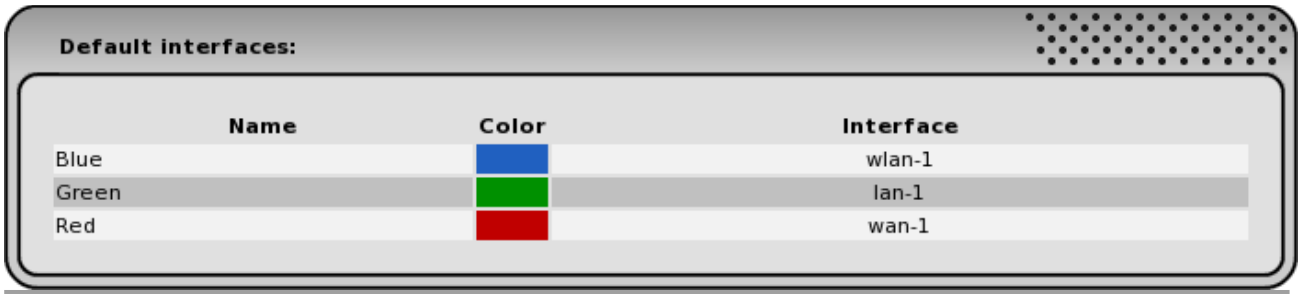
Todas las interfaces personalizadas que haya creado están listadas en la segunda sección.

Para borrar una interfaz personalizada, pulse el icono de la *papelera*. Para editarla, pulse en el icono del *lápiz amarillo*.

2.6.9.3. Interfaces por defecto

Las interfaces por defecto en su IPCop se muestran en la tercera sección.

Figura 2.56. Interfaces por defecto



2.6.10. Página administrativa de reglas del cortafuegos

Todas las reglas son una combinación de origen, destino y un servicio de destino. La excepción es el reenvío de puertos, como se ve más abajo.

2.6.10.1. Añadir una regla nueva

En la primera sección, pulse uno de los botones para añadir una regla para una tarea en particular.

Figura 2.57. Añadir una regla nueva

El origen es una combinación de interfaz(es) y dirección(es).

El destino es una combinación de interfaz(es) y dirección(es).

Las reglas pueden ser las acciones Aceptar, Descartar y Rechazar.

El registro es una opción que se puede activar para cada regla.

Cuando el Modo Avanzado está activado, es posible añadir un puerto de origen a la regla.

Cuando el Modo Avanzado está activado, también es posible añadir una franja de tiempo en la que la regla está activa.

2.6.10.2. Tráfico saliente

Controla el tráfico desde las redes internas a la externa (ROJA = Internet). Si la política es 'semi-abierta' o 'cerrada' necesitará crear una regla para todo tráfico que desee permitir.

2.6.10.3. Acceso a IPCop

Controla el tráfico desde las redes internas a IPCop. Si la política es 'cerrada' necesitará crear una regla para cualquier servicio de IPCop que desee utilizar (incluyendo servicios como DHCP, DNS, Time, etc.).

Si quiere añadir una regla para evitar el registro de los servicios Netbios de su red Verde, debería hacerlo en esta sección.

2.6.10.4. Tráfico interno

Controla el tráfico *entre* redes internas. Por ejemplo, crea un pinhole entre las redes Naranja y Verde.

Este botón sólo estará visible si tiene una interfaz Azul y/o Naranja.

2.6.10.5. Reenvío de puertos

Reenvía el tráfico desde el exterior (ROJA, Internet) a una red interna.

Los reenvíos de puertos son especiales. La interfaz de origen siempre es Roja. El destino está dividido entre un destino 'intermedio'; la dirección externa de IPCop o la dirección alias, y un destino 'final', que es el servidor interno que necesita ser accedido desde el exterior.

2.6.10.6. Acceso externo a IPCop

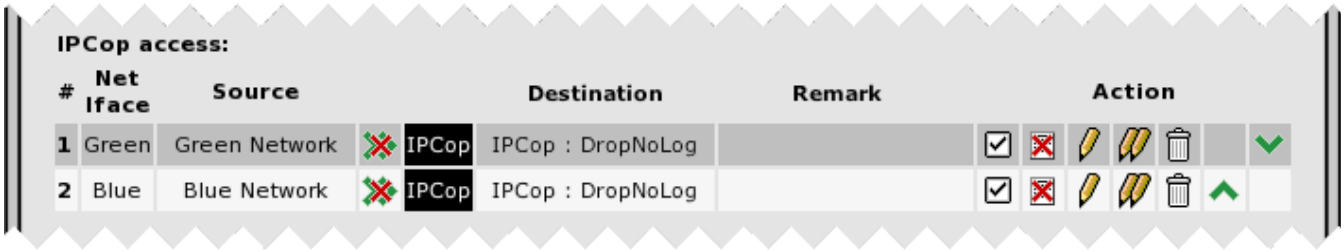
Controla el tráfico desde la interfaz Roja a IPCop.

2.6.10.7. Reglas activas

Cualquier regla que haya creado está listada en la segunda sección.

En el ejemplo de abajo, el Grupo de Servicios *DropNoLog* que se creó anteriormente, se aplica a las redes Verde y Azul, y el registro está desactivado.

Figura 2.58. Ejemplo de una regla



Para activar o desactivar una regla, pulse sobre la casilla en la columna Acción de la regla concreta que quiere activar o desactivar. El icono cambia a una casilla vacía cuando la regla está desactivada. Pulse en la casilla para cambiar el estado.

Para activar o desactivar el registro en una regla, pulse en el icono *Registro* de esa regla. Un icono con una cruz roja indica que el registro está desactivado. Pulse en el icono de nuevo para cambiar este ajuste.

Para editar una regla, pulse en su icono del *lápiz amarillo*. Los ajustes se mostrarán en el formulario de entrada. Haga sus cambios y pulse el botón Guardar del formulario.

Para copiar una regla, pulse en el icono de los *dos lápices amarillos* de la regla que desea copiar. Los ajustes se mostrarán en el formulario de entrada. Haga sus cambios y pulse el botón Guardar.

Para borrar una regla, pulse en su icono de la *papelera*.

Cuando tenga más de una regla en una sección, puede cambiar el orden de las reglas pulsando las flechas *Arriba* o *Abajo* en la columna Acción.

2.7. Menú VPNs

El menú VPNs contiene páginas que controlas las Redes Privadas Virtuales, que permiten a IPCop conectar dos (o más) redes directamente entre ellas sobre otra red, como por ejemplo Internet. Para llegar a estas páginas, seleccione VPNs en la barra de pestañas de la parte superior de la pantalla. Aparecerán las siguientes opciones en un menú desplegable:

- IPsec
- OpenVPN
- CA (Autoridades Certificadoras)

2.7.1. Redes Privadas Virtuales (VPNs)

Las Redes Privadas Virtuales o VPNs permiten conectar dos redes directamente entre ellas sobre otra red, como Internet. Todos los datos son transmitidos de forma segura a través de un túnel encriptado, oculto a ojos de los fisgones. De forma similar, un solo ordenador también se puede conectar a otra red empleando las mismas capacidades. Uno de los protocolos usados para crear VPNs es el conocido como IPsec. Otro es SSL/TLS, empleado por OpenVPN.

IPCop puede establecer VPNs fácilmente con otros servidores IPCop. IPCop también puede interoperar con casi cualquier producto que emplee IPsec o OpenVPN. Esto es completamente opcional, así que puede ignorar esta sección con seguridad si no desea hacer uso de esta prestación. IPCop puede usar tanto IPsec como OpenVPN al mismo tiempo.

La mayoría de sistemas operativos modernos tienen soporte para IPsec y/o OpenVPN. Esto incluye Windows, Macintosh OSX, Linux y la mayoría de las variantes de Unix. Desafortunadamente, las herramientas necesarias para proporcionar este soporte varían enormemente y pueden ser difíciles de configurar.

Nota

Los *relojes* y *zonas horarias* en cada lado de un túnel VPN deben estar *actualizados* antes de configurar o iniciar una VPN.

2.7.1.1. Red-a-Red

Las VPNs Red-a-Red enlazan dos o más redes privadas a través de Internet, creando un "túnel" IPsec. En una VPN Red-a-Red, al menos una de las redes involucradas debe conectarse a Internet con un cortafuegos IPCop. La otra red puede estar conectada con un cortafuegos IPCop, u otro enrutador o cortafuegos con soporte IPsec. Estos enrutadores/cortafuegos tienen direcciones IP públicas asignadas por un ISP y con toda probabilidad están usando NAT (Network Address Translation), de ahí el término Red-a-Red.

Nota

Las VPNs Red-a-Red sólo se pueden crear usando IPsec. OpenVPN Red-a-Red aún no está implementado.

2.7.1.2. Host-a-Red

Una conexión Host-a-Red es cuando IPCop está en uno de los lados del túnel VPN y un usuario remoto o móvil está al otro lado. El usuario móvil probablemente sea un ordenador portátil con una dirección IP pública dinámica asignada por un ISP, de ahí los términos Host-a-Red o Roadwarrior.

Si se desea, se puede crear una VPN entre máquinas inalámbricas en su red AZUL y un cortafuegos IPCop. Esto asegura que el tráfico en su red AZUL no puede ser interceptado con sniffers inalámbricos.

2.7.2. Métodos de Autenticación

Es necesario tener una clave/contraseña/frase precompartida o un certificado X.509 antes de intentar configurar una conexión VPN Red-a-Red o Roadwarrior. Estos son métodos de autenticación, que identifican al usuario que intenta acceder a la VPN. Serán necesarios en la fase de configuración de la VPN.

2.7.2.1. Clave precompartida

El método de autenticación con clave precompartida o PSK es un método muy simple que permite configurar conexiones VPN rápidamente. Para este método, introduzca una frase de autenticación. Ésta puede ser cualquier cadena de caracteres - similar a una contraseña. Esta frase debe estar disponible para la autenticación en IPCop y en el cliente VPN.

El método PSK conlleva menos pasos que la autenticación con certificado. Puede emplearse para comprobar la conectividad de una VPN y para familiarizarse con el procedimiento de establecer una conexión VPN.

El método de clave precompartida no debería utilizarse con conexiones Roadwarrior, ya que todos los roadwarrios deben usar la misma clave precompartida.

2.7.2.2. Certificados X.509

Los certificados X.509 son una forma muy segura de conectar servidores VPN. Para implementar certificados X.509 debe generar o configurar los certificados en IPCop o usar otra autoridad de certificación en su red.

Terminología X.509

Los certificados X.509 de IPCop y muchas otras implementaciones se manipulan y controlan con OpenSSL. SSL (Secure Sockets Layer) tiene su propia terminología.

Los certificados X.509, dependiendo del tipo, pueden contener claves de encriptación públicas y privadas, contraseñas e información acerca de la entidad a la que hacen referencia. Estos certificados están destinados a ser validados por Autoridades de Certificación (Autoridades Certificadoras) o CAs. Cuando se usan en navegadores web, los certificados de las mayores CAs, de pago, están compilados en el propio navegador. Para validar un certificado de host, se pasa el certificado a la CA apropiada para realizar la validación. En redes privadas o hosts únicos, la CA puede residir en un host local. En el caso de IPCop, es el propio cortafuegos IPCop.

Las peticiones de certificación son peticiones de certificados X.509 que se pasan a las CAs. Las CAs generan un certificado X.509 firmando la petición. Ésto es devuelto a la entidad solicitante como certificados X.509. Este certificado será reconocido por la CA, ya que ella lo firmó.

Verá que los certificados X.509 y las peticiones se pueden almacenar en su disco duro en tres formatos diferentes, habitualmente identificados por su extensión. El formato PEM es el formato por defecto de OpenSSL. Puede contener toda la información asociada con certificados en formato imprimible. El formato DER sólo contiene la información necesaria, y ninguna información adicional X.509. Este es el formato por defecto para la mayoría de los navegadores. El formato PEM envuelve cabeceras alrededor de las claves del formato DER. Los certificados PKCS#12, PFK o P12 contienen la misma información que los archivos PEM en formato binario. Usando el comando **openssl**, los archivos PEM y PKCS#12 se pueden transformar unos en otros.

Para usar un certificado, debe importarlo también en la CA del otro lado. La implementación IPsec de IPCop contiene su propia CA. Las CAs también pueden correr en máquinas roadwarrior.

Si la implementación IPsec del roadwarrior no tiene capacidades CA, puede generar una petición de certificado, importarlo a IPCop para que IPCop pueda firmarlo, exportar el certificado resultante e importarlo en el software IPsec del roadwarrior original.

2.7.3. Página administrativa de Configuración IPsec

Para configurar una VPN con IPsec, haga lo siguiente:

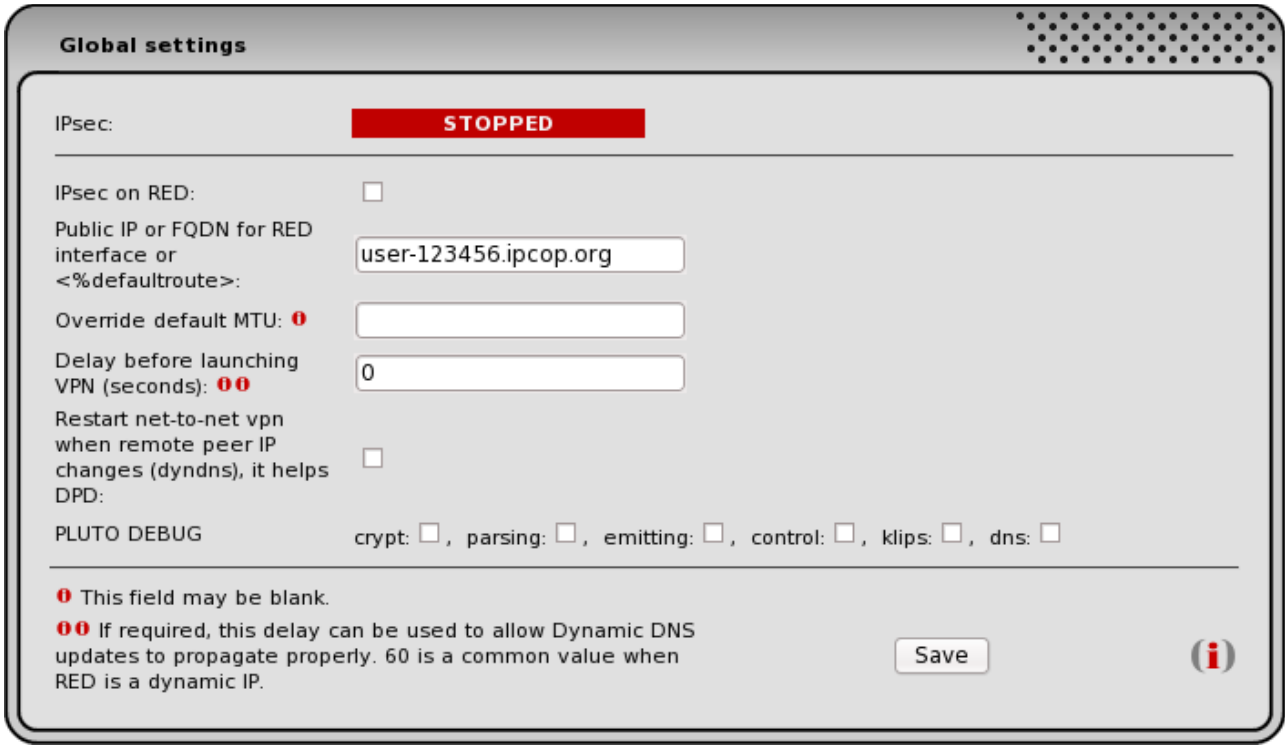
1. Cree una Autoridad Certificadora.
2. Active IPsec en la(s) interfaz(es) de su elección en la sección Ajustes Globales.
3. Añada o bien una conexión Host-a-Red (Roadwarrior) o bien una conexión Red-a-Red.
4. Siguiente elemento...

5. Siguiente elemento...

2.7.3.1. Ajustes Globales

La primera línea en la sección de Ajustes Globales indica si el servidor **IPsec** está parado o corriendo.

Figura 2.59. Ajustes globales



IPsec en ROJA. Marque esta casilla para activar el servidor IPsec en ROJA.

IPsec en AZUL. Sólo visible si tiene configurada una interfaz AZUL. Marque esta casilla para activar el servidor IPsec en AZUL.

IP pública o FQDN de la interfaz ROJA o <%defaultroute>. Introduzca los detalles del servidor IPsec, su FQDN o la dirección IP pública de la interfaz roja. Si está utilizando un servicio de DNS dinámico, aquí debería usar su nombre DNS dinámico.

VPNs y DNS dinámico

Si su ISP cambia su dirección IP, tenga en cuenta que las VPNs Red-a-Red pueden necesitar ser reiniciadas desde ambos extremos del túnel. Los roadwarriors también tendrán que reiniciar sus conexiones en tal caso.

Saltar MTU por defecto - opcional. El MTU (Maximum Transmission Units) es el tamaño máximo del datagrama en bytes que puede ser enviado sin fragmentar sobre un camino de red concreto.

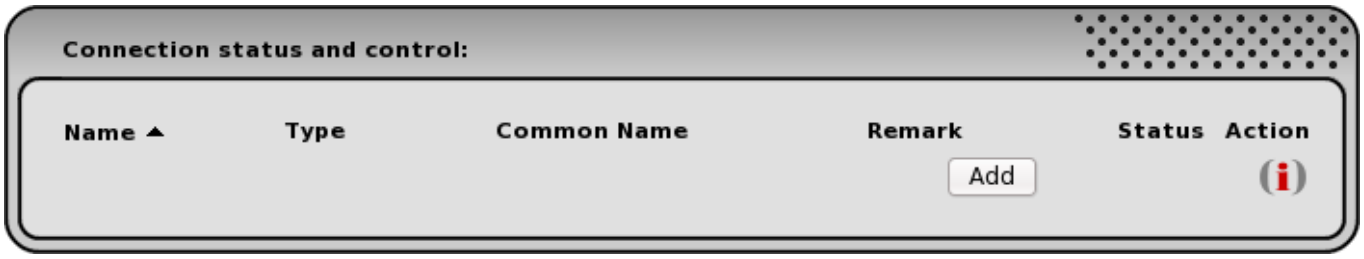
Retraso antes de lanzar la VPN (segundos). Si tiene una dirección IP pública fija en ROJA, debería mantener el valor 0. Si utiliza un servicio de DNS dinámico, debería usar un valor mínimo de 60 segundos para que la entrada de DNS dinámico tenga tiempo suficiente de propagarse a todos los servidores DNS.

Reiniciar VPN Red-a-Red cuando la IP remota cambie... Reinicia la VPN Red-a-Red cuando la IP remota cambia (dyndns). Esto ayuda al Dead Peer Detection (DPD). Añadir contenido...

PLUTO DEBUG. Varias opciones de depuración que pueden ayudar a resolver problemas. Utilíce-lo con cuidado, los muchos mensajes de registro adicionales suelen ser confusos.

2.7.3.2. Estado y control de la conexión

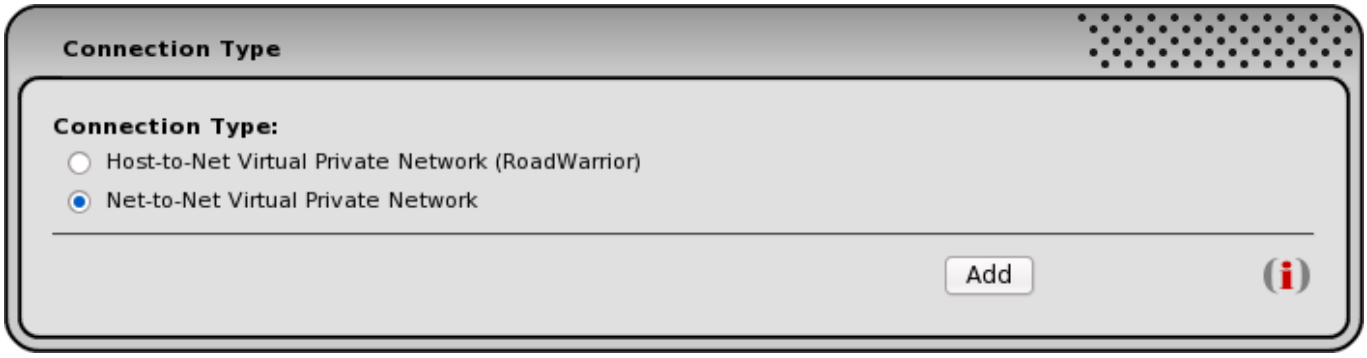
Figura 2.60. Ventana de Estado y control de la conexión: Vista inicial



Para crear una conexión VPN IPsec utilice el botón Añadir. Aparecerá la página de tipo de conexión VPN.

2.7.3.3. Tipo de conexión

Figura 2.61. Selección del tipo de conexión



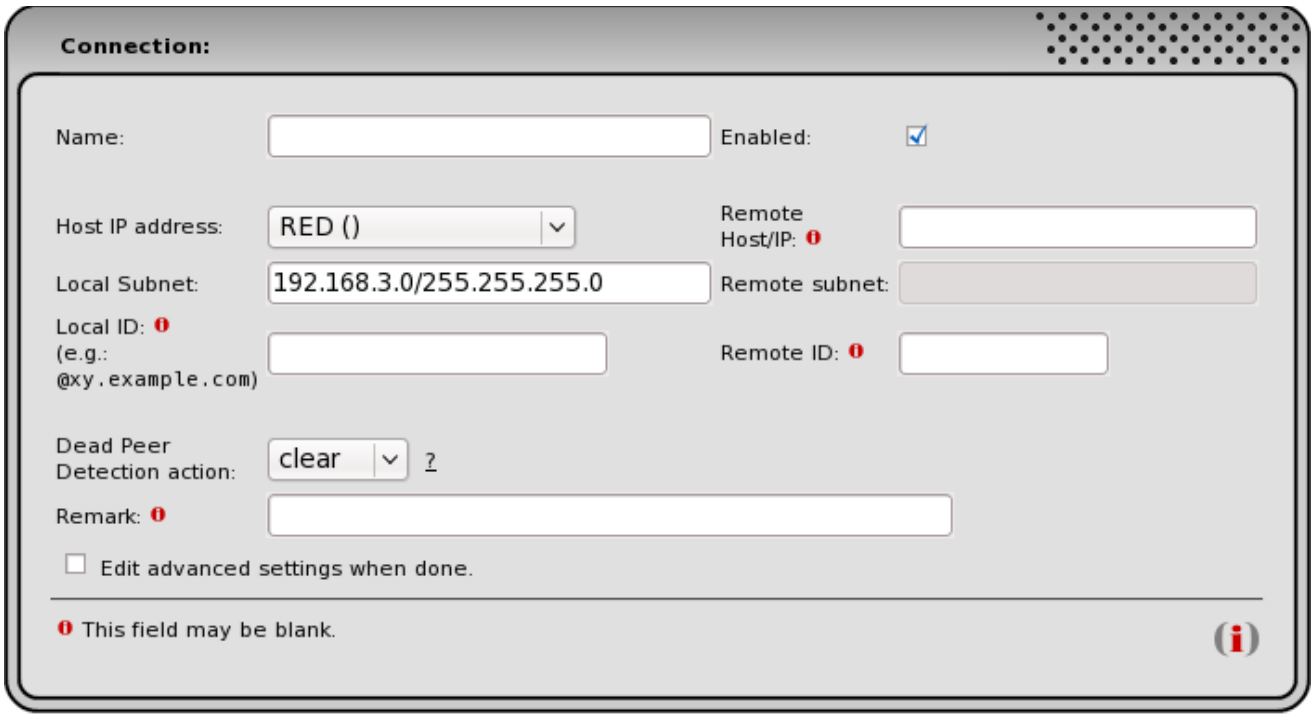
Seleccione VPN Host-a-Red (Roadwarrior) para usuarios móviles que necesitan acceso a la red VERDE o VPN Red-a-Red para dar a usuarios en otra red acceso a su red VERDE y dar a usuarios de su red VERDE acceso a la otra red.

Elija el tipo de conexión que desea crear y pulse el botón Añadir.

La siguiente página que aparece contiene dos secciones. La sección Conexión variará dependiendo del tipo de conexión que esté añadiendo. La sección Autenticación será igual.

2.7.3.4. Conexión Host-a-Red

Figura 2.62. Conexión Host-a-Red



Nombre. Un nombre simple (sólo minúsculas, sin espacios) para identificar esta conexión.

Activado. Marque la casilla Activado para activar esta conexión.

Dirección IP del host. Escribir contenido...

Host remoto/IP - opcional. Introduzca la dirección IP fija del servidor IPsec de la red remota. También puede introducir el FQDN del servidor remoto. Si el servidor remoto está usando un servicio de DNS dinámico, puede que tenga que reiniciar IPsec si su dirección IP cambia. Hay varios scripts disponibles en los grupos de noticias de IPCop que harán esto por usted.

Subred Local. Subred Local es por defecto su red VERDE. Si lo desea, puede crear una subred de su red VERDE para limitar el acceso roadwarrior a su red VERDE.

ID local - opcional. Escribir contenido...

ID remota - opcional. Escribir contenido...

Acción de Dead Peer Detection. Elija entre “limpiar”, “mantener” o “reiniciar”.

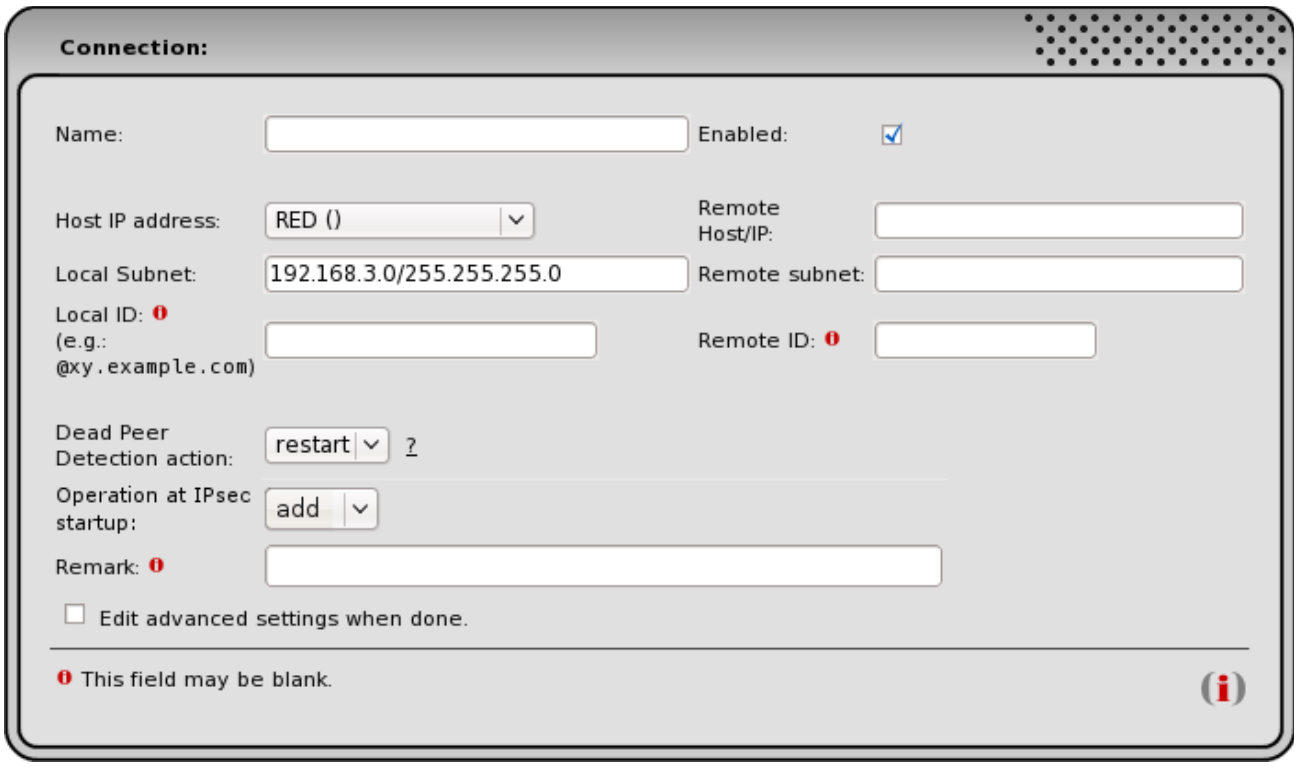
Openswan recomienda en su archivo README.DPD que se use “mantener” para túneles definidos estáticamente, y “limpiar” para túneles roadwarrior.

Reseña - opcional. El campo Reseña le permite añadir un comentario opcional que aparecerá en la ventana de conexión VPN de IPCop para esta conexión.

Editar ajustes avanzados al terminar. Marque la casilla Editar ajustes avanzados al terminar si necesita modificar los ajustes por defecto de IPCop para IPsec.

2.7.3.5. Conexión Red-a-Red

Figura 2.63. Conexión Red-a-Red



Nombre. Un nombre simple (sólo minúsculas, sin espacios) para identificar esta conexión.

Activado. Marque la casilla Activado para activar esta conexión.

Dirección IP del host. Escribir contenido...

Host remoto/IP. Introduzca la dirección IP fija del servidor IPsec de la red remota. También puede introducir el FQDN del servidor remoto. Si el servidor remoto está usando un servicio de DNS dinámico, puede que tenga que reiniciar IPsec si su dirección IP cambia. Hay varios scripts disponibles en los grupos de noticias de IPCop que harán esto por usted.

Subred Local. Subred Local es por defecto su red VERDE. Si lo desea, puede crear una subred de su red VERDE para limitar el acceso roadwarrior a su red VERDE.

Subred remota. Introduzca la dirección de red y la máscara de red la red remota en el mismo formato que el campo Subred Local. Esta red debe ser diferente a la Subred Local ya que IPsec configura entradas en la tabla de rutas para enviar paquetes IP a la red remota correcta.

ID local - opcional. Escribir contenido...

ID remota - opcional. Escribir contenido...

Acción de Dead Peer Detection. Elija entre “limpiar”, “mantener” o “reiniciar”.

Openswan recomienda en su archivo README.DPD que se use “mantener” para túneles definidos estáticamente, y “limpiar” para túneles roadwarrior.

Operación al iniciar IPsec. Elija entre “añadir”, “enrutar” o “iniciar”.

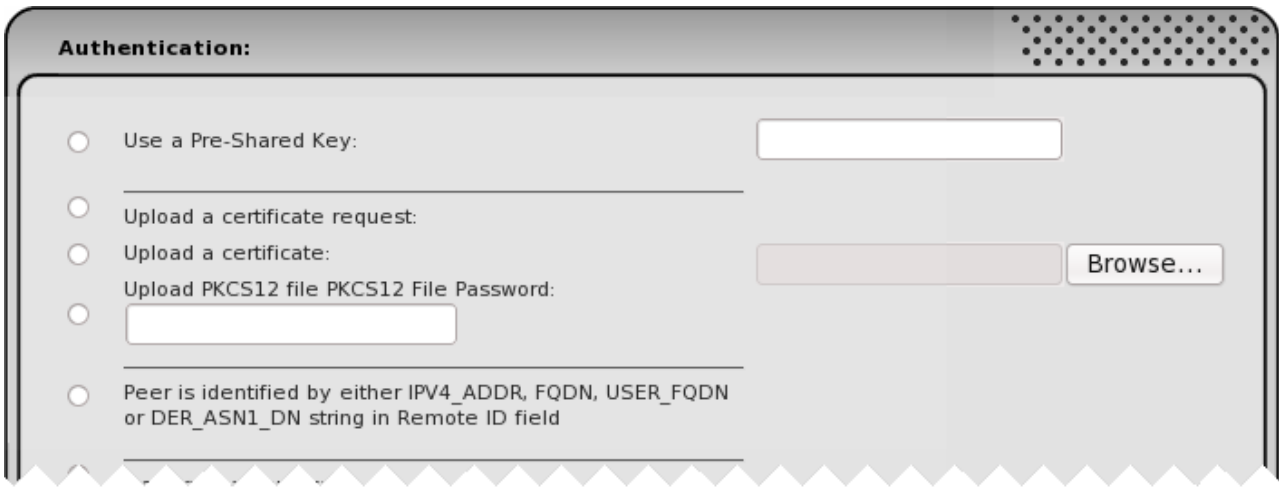
Reseña - opcional. El campo Reseña le permite añadir un comentario opcional que aparecerá en la ventana de conexión VPN de IPCop para esta conexión.

Editar ajustes avanzados al terminar. Marque la casilla Editar ajustes avanzados al terminar si necesita modificar los ajustes por defecto de IPCop para IPsec.

2.7.3.6. Autenticación

La segunda sección de la página web trata sobre la autenticación. En otras palabras, así es como este IPCop se asegurará de que el túnel establecido por ambas partes de la interfaz está hablando a su opuesto. IPCop ha hecho todo lo posible para soportar certificados tanto PSK como X.509. Hay cuatro elecciones, mutuamente excluyentes, que se pueden emplear para autenticar una conexión.

Figura 2.64. Autenticación

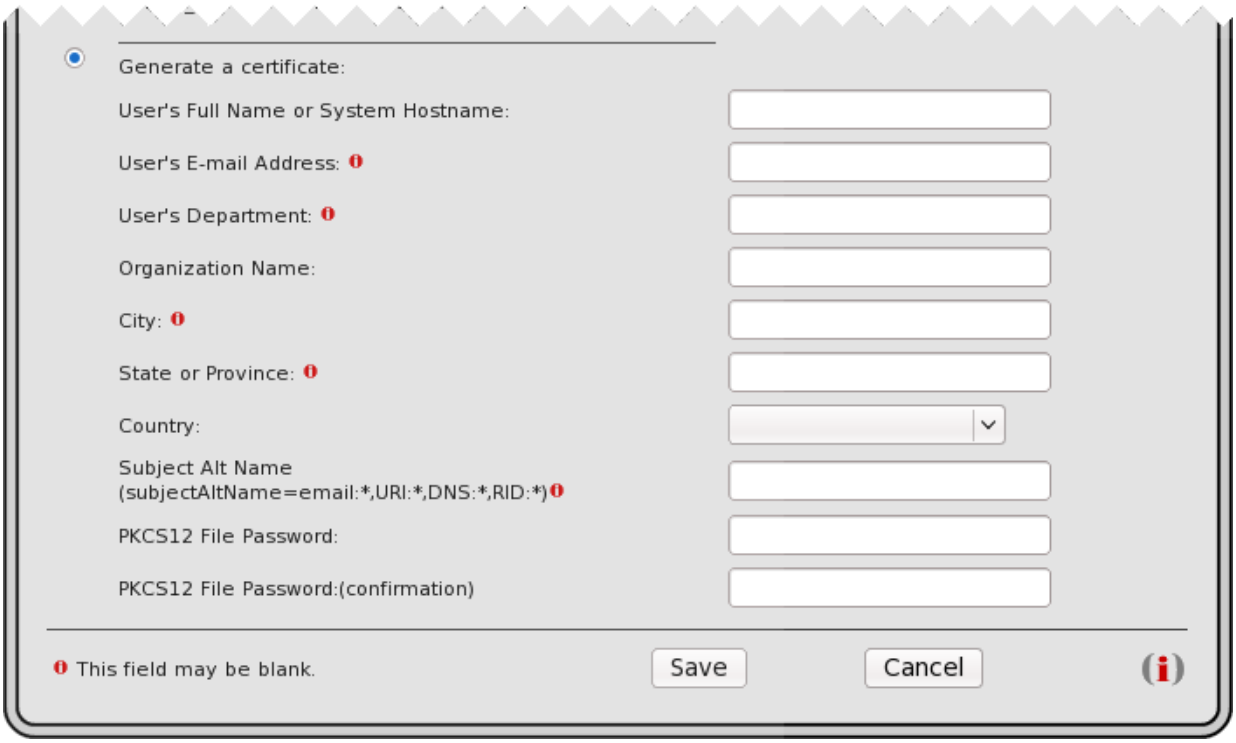


Utilizar una clave precompartida. Introduzca una frase de paso que se usará para autenticar al otro lado del túnel. Escoja esto si quiere una VPN Red-a-Red simple. También puede emplear PSKs mientras experimenta en la creación de VPNs. *No utilice PSKs para autenticar túneles de roadwarriors.*

Subir petición de certificado. Algunas implementaciones IPsec de roadwarrior no tienen su propia CA. Si quieren utilizar la CA integrada en IPCop, pueden generar lo que se llama una petición de certificado. Esto es un certificado X.509 parcial que debe ser firmado por una CA para ser un certificado completo. Durante la subida de la petición de certificado, la petición es firmada y el nuevo certificado estará disponible en la página web principal de VPNs.

Subir un certificado. En este caso, el par IPsec tiene una CA disponible para usar. Se deben subir tanto el certificado del par como el certificado del host.

Figura 2.65. Continuación de autenticación



Generar un certificado. En este caso, el par IPsec podrá ofrecer un certificado X.509, pero no tiene la capacidad ni siquiera de generar una petición de certificado. En este caso, rellene los campos requeridos. Los campos opcionales están indicados con puntos rojos. Si este certificado es para una conexión Red-a-Red, el campo Nombre de usuario completo o Nombre del sistema pueden ser el FQDN de Internet del par. El nombre de organización opcional es para aislar diferentes porciones de una organización del acceso a la red VERDE completa haciendo subredes de la Subred local en el apartado de definición de conexión de esta página web. El campo Contraseña del archivo PKCS12 asegura que los certificados de host generados no puedan ser interceptados y comprometidos mientras se transmiten al par IPsec.

2.7.4. Página administrativa de Configuración de OpenVPN

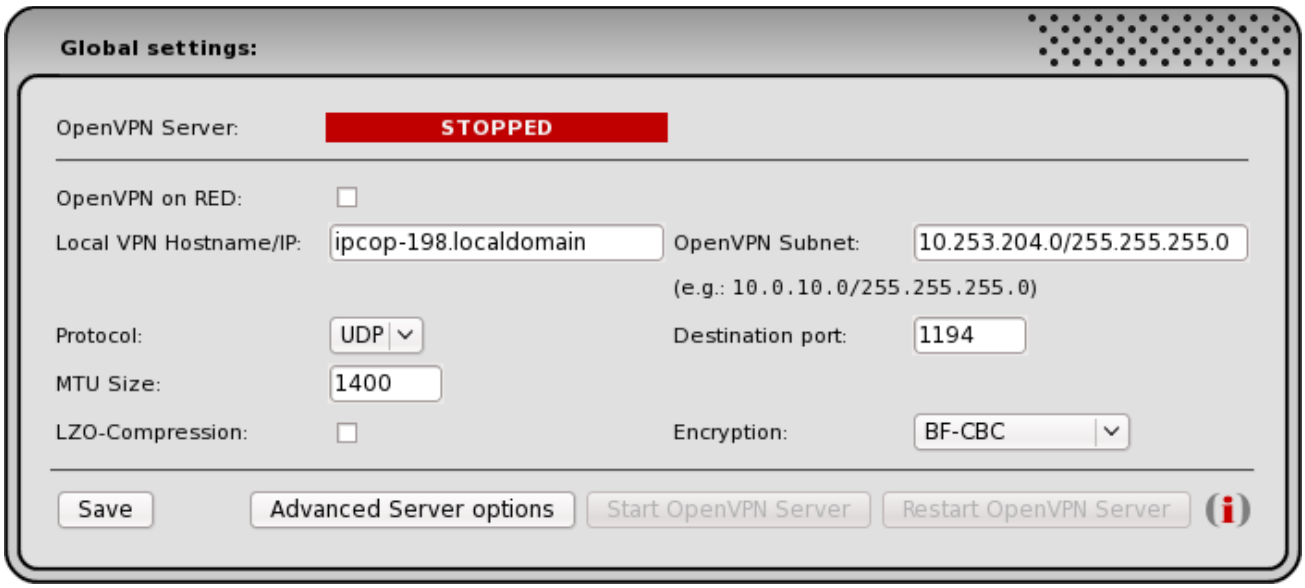
Nota

Antes de poder iniciar y utilizar el servidor OpenVPN necesita crear una Autoridad Certificadora.

2.7.4.1. Ajustes globales

La primera línea en la sección de Ajustes indica si el servidor **OpenVPN** está parado o corriendo.

Figura 2.66. Ajustes globales



OpenVPN en ROJA. Marque esta casilla para activar el servidor OpenVPN en ROJA.

OpenVPN en AZUL. Sólo visible si tiene una interfaz AZUL configurada. Marque esta casilla para activar el servidor OpenVPN en AZUL.

IP/nombre de host VPN local. Introduzca el FQDN o la dirección IP pública de la interfaz ROJA. Si está usando un servicio de DNS dinámico, debería usar su nombre de DNS dinámico aquí.

Subred OpenVPN. Escribir contenido...

Protocolo. Elija UDP (por defecto) o TCP. Del manual de OpenVPN:

OpenVPN está diseñado para funcionar de manera óptima sobre UDP, aunque se ofrece capacidad TCP para situaciones
en las que no se puede usar UDP. En comparación con UDP, TCP será normalmente algo menos ef iciente y menos robusto cuando se
usa sobre redes poco fiables o congestionadas.

En este artículo se describen algunos problemas con los túneles IP sobre TCP:

http://sites.inka.de/sites/bigred/devel/tcp-tcp.html

Puerto de destino. El número de puerto TCP/UDP utilizado. Por defecto es el 1194, la asignación de número de puerto oficial de IANA para OpenVPN.

Tamaño MTU. El MTU (Maximum Transmission Units) es el tamaño máximo del datagrama en bytes que puede ser enviado sin fragmentar sobre un camino de red concreto. OpenVPN necesita que los paquetes en los canales de control y de datos se envíen sin fragmentar.

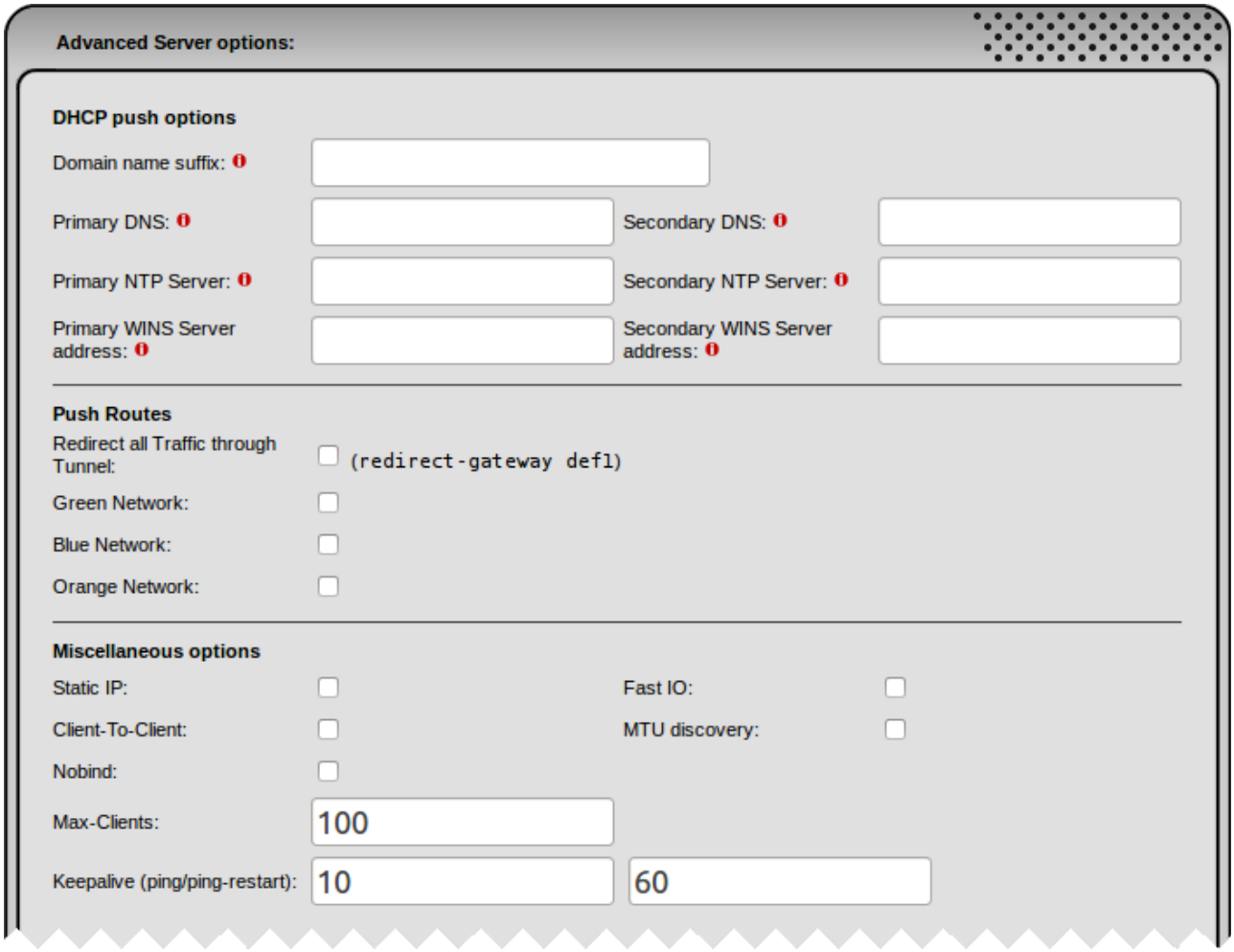
Compresión LZO. Utilizar compresión LZO.

Encriptación. OpenVPN puede utilizar varios algoritmos para encriptar paquetes. BF-CBC (Blow-fish in Cipher Block Chaining), por defecto, es a la vez rápido y muy seguro.

2.7.4.2. Opciones avanzadas del servidor

Es importante que seleccione la ruta correcta a entregar a los clientes, en la página de Opciones avanzadas del servidor.

Figura 2.67. Opciones avanzadas del servidor (arriba)



Opciones 'push' DHCP. El servidor OpenVPN puede entregar opciones DHCP como direcciones de servidores DNS y WINS a los clientes. Los clientes Windows pueden aceptar las opciones DHCP entregadas de forma nativa, mientras que los clientes no Windows pueden aceptarlas con algo de configuración adicional. Vea el OpenVPN HowTo para más detalles.

Sufijo de nombre de dominio Ponga un sufijo DNS específico de esta conexión, por ejemplo `local.ejemplo.org` Esto es opcional.

DNS primario/secundario Añada una dirección de un servidor de nombres de dominio, por ejemplo `192.168.1.1`

Éstos son opcionales, pero cuando se usa **puerta de redirección**, los clientes de OpenVPN enrutarán las peticiones DNS a través de la VPN, y el servidor VPN tiene que manejarlas. Esto se puede lograr entregando una dirección de servidor DNS a los clientes que se conectan, que reeplazan los ajustes normales de servidores DNS durante el tiempo que esté activa la VPN.

Servidores NTP primario y secundario Añada aquí la dirección IP de un servidor NTP, por ejemplo `192.168.1.1` para pasarla a los clientes. Éstas son opcionales.

Direcciones de servidor WINS primario/secundario Añada aquí la dirección IP de un servidor WINS, por ejemplo `192.168.1.254` para pasarla a los clientes. Éstas son opcionales.

Rutas 'push'. El servidor OpenVPN entrega información de enrutamiento a los clientes. Seleccione la red a la que quiere enrutar el tráfico.

Redireccionar todo el tráfico a través del túnel Active esto cuando quiera tunelar todo el tráfico de un cliente a través de la VPN, incluyendo el tráfico general de navegación por Internet. El cliente sufrirá un impacto en las prestaciones cuando todo el tráfico tiene que pasar a través del servidor OpenVPN.

Esto añade `push "redirect-gateway def1"` al archivo de configuración del servidor.

Red Verde Marque esta casilla para enrutar el tráfico a la red Verde.

Red Azul Esta casilla sólo estará visible si tiene una interfaz Azul. Marque esta casilla para enrutar el tráfico a la red Azul.

Red Naranja Esta casilla sólo estará visible si tiene una interfaz Naranja. Marque esta casilla para enrutar el tráfico a la red Naranja.

Nota

Las Redes disponibles están **desactivadas** por defecto.

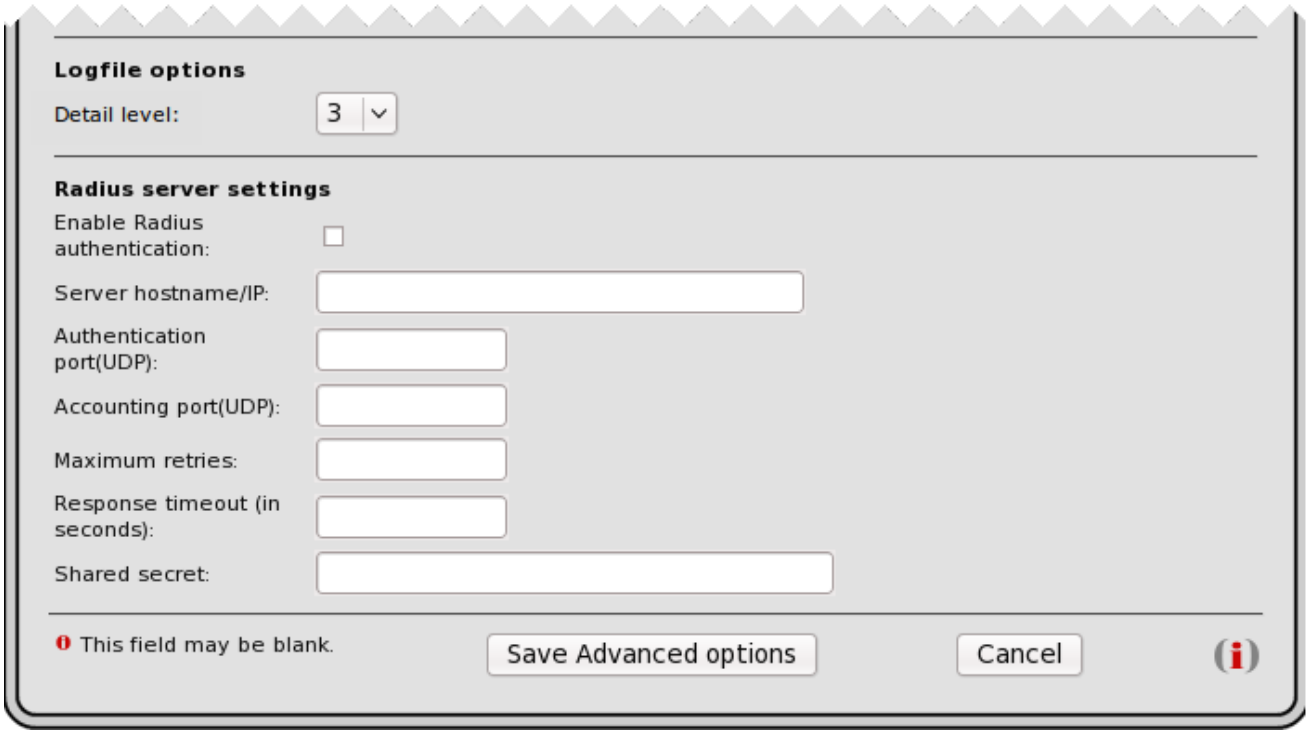
Opciones varias. Escribir contenido...

Escribir contenido...

Máximo de clientes Limita el servidor a un número *n* de clientes concurrentes. El valor por defecto es 100.

Keepalive Los valores por defecto son 10 y 60.

Figura 2.68. Opciones avanzadas del servidor (abajo)



Opciones de archivo registro. Seleccione el nivel de detalle del archivo de registro del menú desplegable Nivel de detalle. 0 es no registrar nada excepto errores fatales. 1 es el mínimo nivel de registro y 11 es el nivel más alto.

Ajustes del servidor Radius. Escribir contenido...

Escribir contenido...

2.7.4.3. Estado y control de clientes

El botón Añadir estará desactivado hasta que los ajustes se hayan guardado.

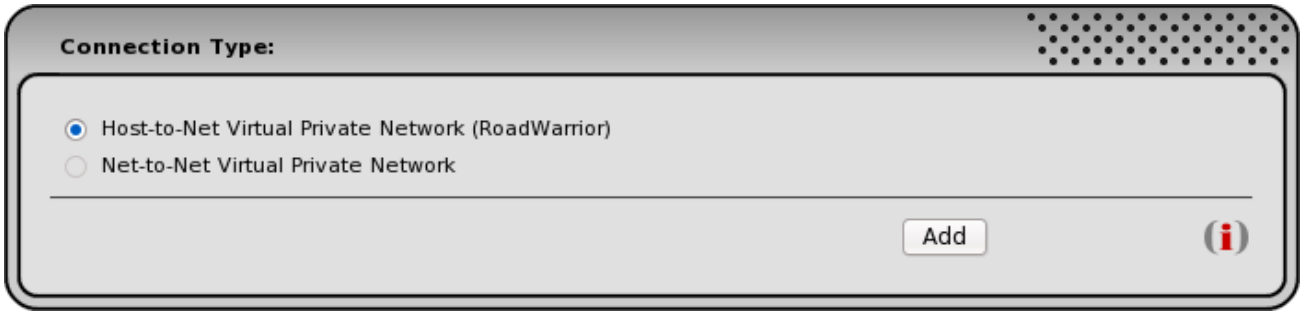
Figura 2.69. Estado y control de clientes

2.7.4.4. Tipo de conexión

La única opción por ahora es VPN Host-a-Red. Observe que el botón VPN Red-a-Red se muestra en gris.

Pulse el botón Añadir para continuar.

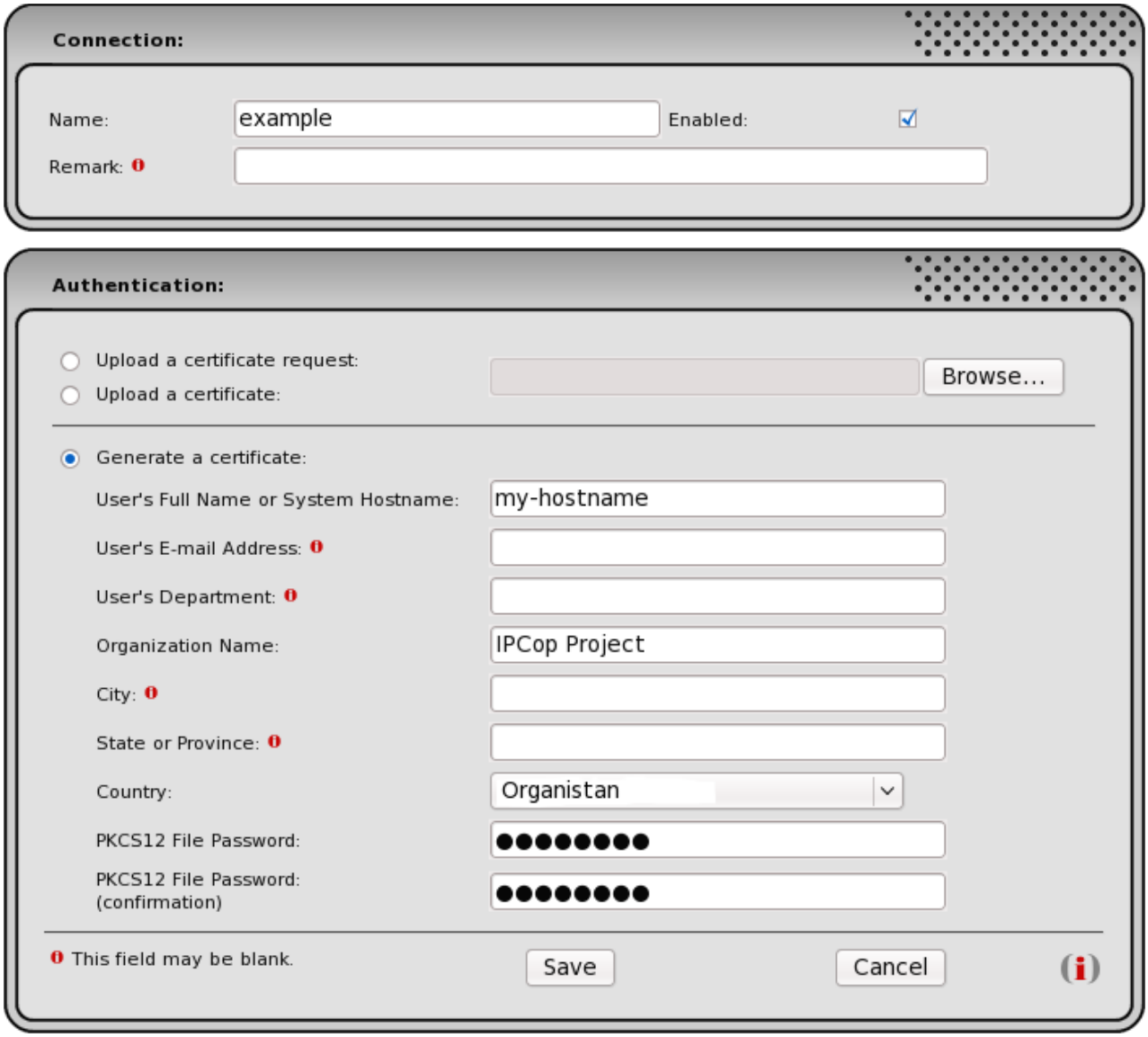
Figura 2.70. Tipo de conexión



2.7.4.5. Conexión y autenticación

Escribir contenido...

Figura 2.71. Conexión



Nombre. El nombre de la conexión sólo puede contener letras y números.

Activado. Marque esta casilla para activar la entrada.

Reseña (opcional). Si lo desea, puede incluir una cadena de texto para describir o identificar la conexión.

Nombre del usuario o del sistema. Escribir contenido...

Dirección de correo del usuario (opcional). Dirección de correo del usuario.

Departamento del usuario (opcional). Este es el nombre del departamento o suborganización. Siguiendo con el ejemplo de la escuela, esto podría ser **`Mi Escuela Elemental`**.

Nombre de la Organización. El nombre de la Organización. Por ejemplo, si este túnel VPN está uniendo escuelas de un mismo distrito, puede querer usar algo como **`Escuelas del Distrito Ejemplo`**.

Ciudad (opcional). La ciudad.

Estado o provincia (opcional). El estado o provincia.

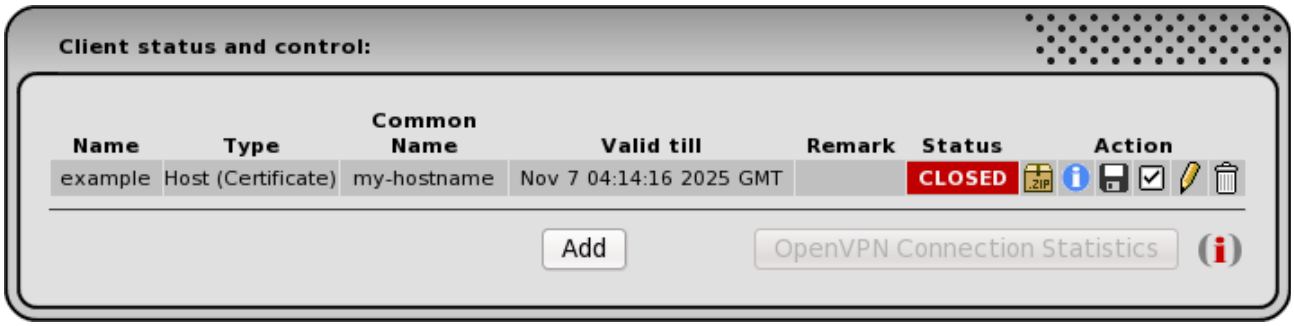
País. Este menú desplegable contiene todos los nombres de países reconocidos en ISO. Úselo para seleccionar el país asociado al túnel.

Contraseña del archivo PKCS12. Escribir contenido...

2.7.4.6. Estado del cliente y control de una conexión

Debajo se muestra un ejemplo de una conexión Host-a-Red con un certificado.

Figura 2.72. Ejemplo de estado del cliente y control



Estado. Cerrado (Parado), Cerrado (Activo) o Abierto.

Icono Descargar paquete del cliente (zip). Escribir contenido...

Icono Mostrar certificado. Escribir contenido...

Icono Descargar certificado. Escribir contenido...

Icono Activado/Desactivado. Cambia la conexión entre activada y desactivada.

Icono Editar. Pinche el icono del *lápiz amarillo* para editar la reseña.

Icono Eliminar. Pinche el icono de la *papelera* para borrar la conexión.

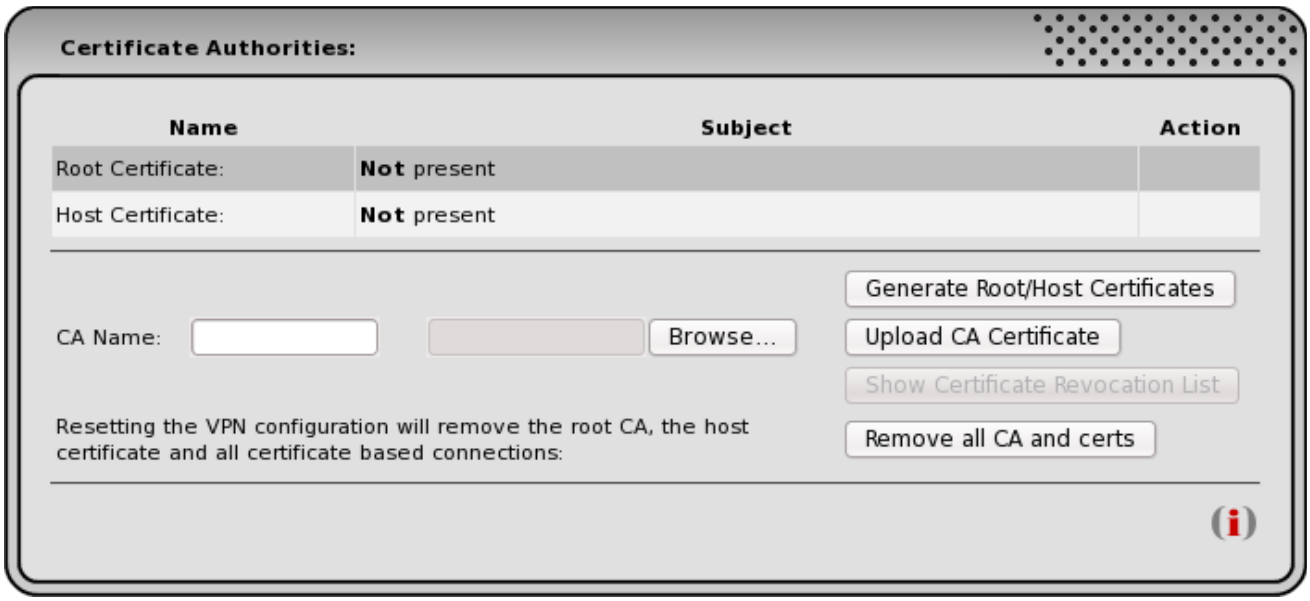
2.7.5. Página administrativa de Autoridades Certificadoras

Es necesario tener una clave/contraseña/frase precompartida o un certificado X.509 antes de intentar configurar una conexión VPN Red-a-Red o Roadwarrior. Estos son métodos de autenticación, que identifican al usuario que intenta acceder a la VPN. Serán necesarios en la fase de configuración de la VPN.

Cree y gestione certificados X.509 en esta página web.

2.7.5.1. Generar certificados Raíz y de Host

Figura 2.73. Ventana de Autoridades Certificadoras: vista inicial

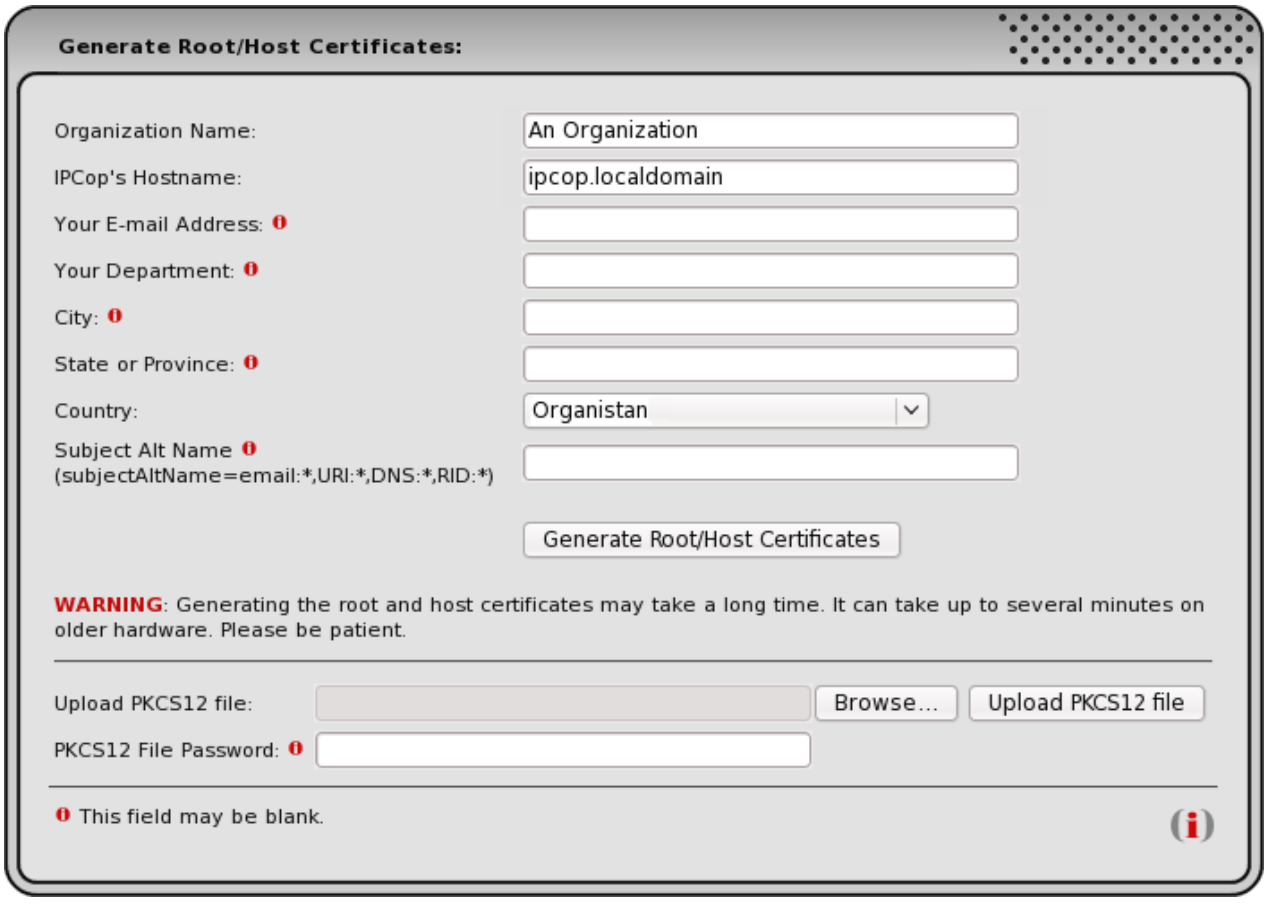


Para crear el certificado Raíz y de Host de IPCop, pinche en el botón Generar certificados Raíz/Host.

Esto abre otra ventana, mostrada más abajo, donde debe introducir algunos detalles para el certificado. Los campos Nombre de Organización, Nombre de IPCop y País son obligatorios (estando el campo Nombre de IPCop normalmente ya rellenado con el nombre de host o la dirección IP de la interfaz Roja).

Una vez que ha introducido toda la información, pulse el botón Generar certificados Raíz/Host de nuevo para generar los certificados X.509 Raíz y de host.

Figura 2.74. Ventana Generar certificados Raíz/Host



Nombre de Organización. El nombre de la organización que quiere que se use en el certificado. Por ejemplo, si este túnel VPN está uniendo escuelas de un mismo distrito, puede querer usar algo como **`Escuelas del Distrito Ejemplo`**.

Nombre de IPCop. Esto debería ser el FQDN de la conexión WAN de su IPCop. Si tiene una IP fija puede introducirla aquí. Si está usando un servicio de DNS dinámico, utilícelo aquí.

Su dirección de correo - opcional. Su dirección de correo, para que la gente pueda saber quién es usted.

Los siguientes tres campos: departamento, ciudad y estado o provincia son opcionales. Puede dejarlos en blanco si lo desea.

Su Departamento - opcional. Este es el nombre del departamento o suborganización. Siguiendo con el ejemplo de la escuela, esto podría ser **`Mi Escuela Elemental`**.

Ciudad - opcional. La ciudad o dirección postal de su máquina.

Estado o provincia - opcional. El estado o provincia asociado con la dirección postal.

País. Este menú desplegable contiene todos los nombres de países reconocidos en ISO. Úselo para seleccionar el país asociado al túnel.

Nombre alternativo - opcional. La extensión nombre alternativo del sujeto permite identidades adicionales que se añadan al sujeto del certificado. Las opciones definidas incluyen una dirección de correo electrónico de Internet, un nombre DNS, una dirección IP, y una URI (uniform resource identifier).

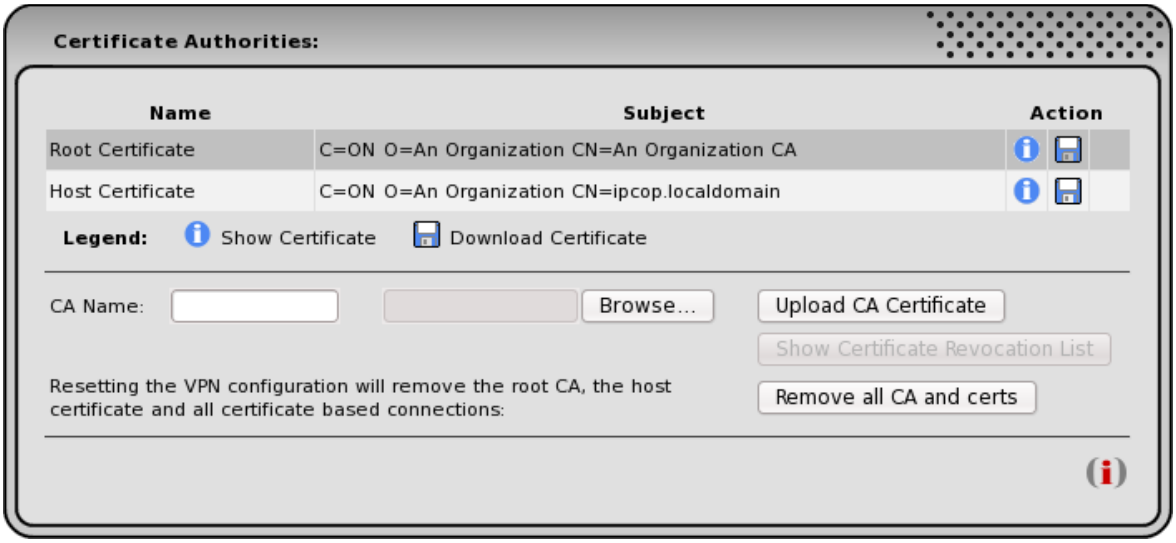
La extensión SubjectAltName está definida en la sección 4.2.1.7 de RFC 3280.

Tras completar el formulario, pinche en el botón Generate Root/Host Certificates para generar los certificados.

Si lo desea, puede generar varios certificados Raíz y de host en un mismo IPCop y luego exportarlos a archivos con formato PKCS12, encriptados con una contraseña. Así puede enviarlos por correo electrónico a sus otros lugares.

Usando la sección Subir archivo PKCS12 de esta página web, puede subir y desencriptar los certificados en una máquina IPCop local.

Figura 2.75. Ventana de Autoridades Certificadoras: con certificados



Para subir una CA desde una máquina remota, déle un nombre en el campo Nombre de CA, que puede ser cualquiera, pero ponga algo con sentido. Si el IPCop remoto es PasarelaCompañía, simplemente llame a la CA **`Compañía`**, y a la conexión **`RedCompañía`** (para una conexión Red-a-Red).

Para ver, descargar o borrar un certificado, pinche en el icono apropiado de la columna Acción.

Pulse el botón Eliminar todas las CAs y certificados para eliminar la CA Raíz, el certificado de host y **todas** las conexiones basadas en certificados.

2.8. Menú Registros

Este grupo de páginas le presenta información de los registros de su servidor IPCop. Para llegar a estas páginas, seleccione Registros de la barra de pestañas en la parte superior de la pantalla. Aparecerán las siguientes opciones en un menú desplagable:

- Ajustes de registros
- Sumario de registros
- Registros del cortafuegos
- Registros del Proxy
- Registros de URL Filter
- Registros del Sistema

Las páginas de registros contienen cinco sub-páginas - Ajustes de registros, Sumario de registros, Registros del Proxy, Registros del cortafuegos y Registros del Sistema. Todos ellos comparten un conjunto de prestaciones de la interfaz para seleccionar la información que desee mostrar, y para exportar esa información a su máquina local. Las listas desplegables Mes: y Día: en el área Ajustes: de la página le permiten seleccionar información de los registros de días y meses anteriores. Cada vez que seleccione una nueva combinación de Mes: y Día:, debe pulsar también el botón Actualizar para que se muestre la información de los registros. Cuando seleciona una sub-página por primera vez, la información mostrada será la de la fecha actual.

El botón << le permite saltar rápidamente al día anterior, y el botón >>, al día siguiente.

La información del registro aparece como una lista en la sección principal de la ventana (normalmente etiquetada como Registro:). Si esa lista es demasiado larga para caber en una ventana de un tamaño razonable, sólo se mostrarán los últimos registros. En ese caso, se activarán los enlaces Más antiguo y Más nuevo en lo alto y en el pie de esta sección de la ventana y podrá emplearlos para recorrer las páginas de la lista de datos del registro.

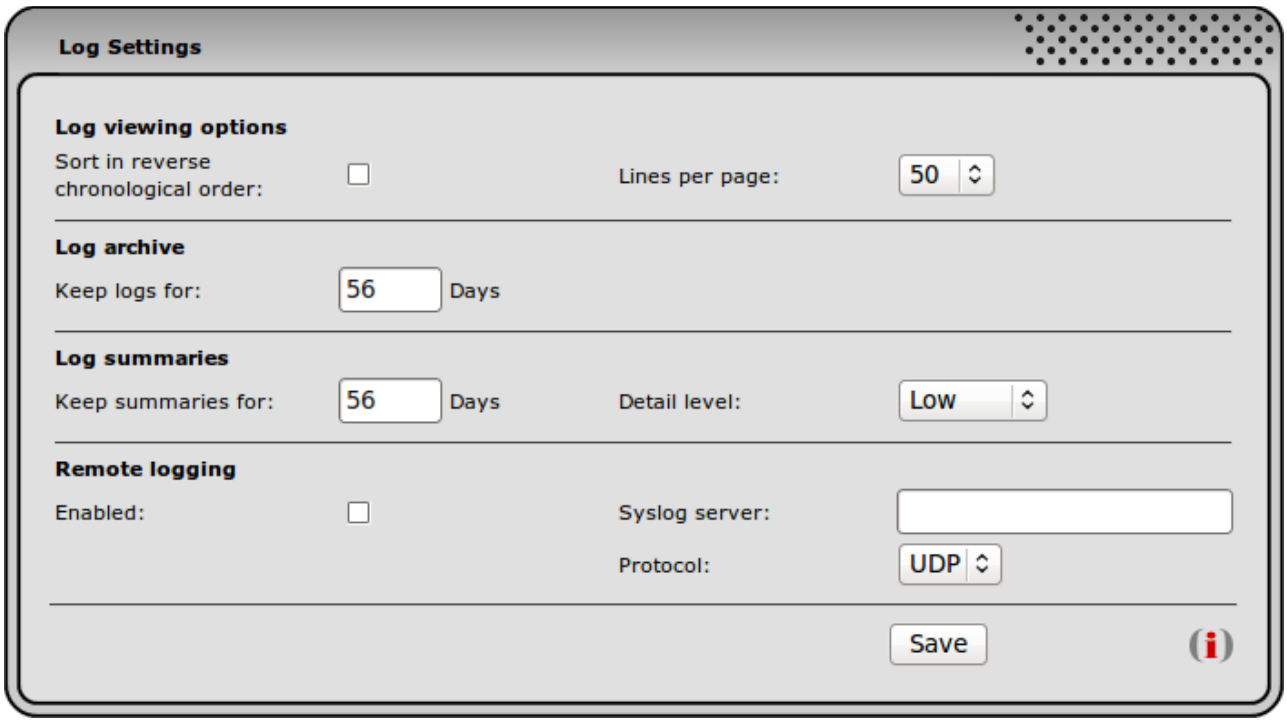
Si presiona el botón Exportar descargará un archivo de texto (`ipcop-<category>-<date>.log`), conteniendo la información de la página de registros actual, del servidor IPCop a su ordenador. Dependiendo de cómo esté configurado su ordenador, presionar el botón Export iniciará un diálogo de descarga de archivo, mostrará el contenido de `ipcop-<category>-<date>.log` en la ventana de su navegador o abrirá el archivo en un editor de texto. En los dos últimos casos puede guardar `ipcop-<category>-<date>.log` como un archivo de texto si lo necesita.

2.8.1. Página administrativa de Ajustes de Registros

Ajustes de registros. Esta página le permite controlar cómo se muestran los registros, especificar el nivel de detalle y durante cuánto tiempo se guardan los sumarios de registros, y controlar el registro remoto.

Pulse el botón Guardar tras realizar cualquier cambio para guardar los ajustes y reinicie el demonio **syslogd**.

Figura 2.76. Ajustes de registros



Orden cronológico inverso. Marque la casilla Orden cronológico inverso si quiere ver los eventos más recientes en la parte superior de una página, en vez de abajo.

Líneas por página. Seleccione el número de entradas del registro que se mostrarán en una página con el menú desplegable Líneas por página. Éste puede variar entre 15 y 500. Tenga en cuenta que un número elevado de líneas necesitará más tiempo para procesarse y mostrarse en hardware lento.

Achivo de registros. Puede elegir durante cuánto tiempo se guardan los registros en IPCop. Por defecto son 8 semanas (56 días), pero puede aumentar o disminuir este período en función de sus necesidades y la cantidad de espacio en disco disponible.

Mantener sumarios durante n días. Puede elegir durante cuánto tiempo se guardan los sumarios de **logwatch** en IPCop. Si tiene poco espacio en disco, reduzca el número de días.

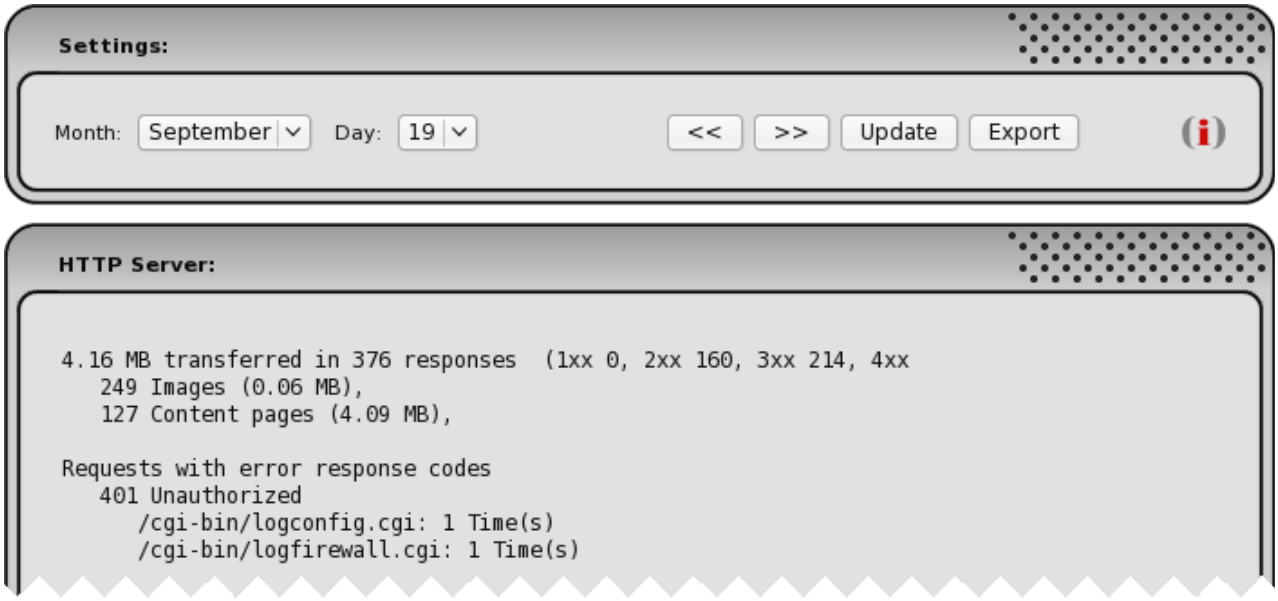
Nivel de detalle. Puede elegir entre los niveles de detalle Bajo, Medio y Alto para los sumarios de **logwatch** desde el menú desplegable Nivel de detalle.

Registro remoto. Seleccione la casilla Activado para permitir registrar en un servidor syslog remoto.

Especifique el FQDN o la dirección IP del servidor remoto en el campo Servidor Syslog proporcionado. Todos los registros se enviarán a ese servidor.

Puede cambiar el protocolo de registro a TCP/514, en vez de UDP/514, si lo nececesita. Por defecto es UDP.

Recuerde pulsar el botón Guardar tras realizar cualquier cambio.



2.8.3. Página de registros del Proxy

Esta página le ofrece la posibilidad de ver los archivos que han sido cacheados por el servidor proxy web de IPCop. El proxy web está inactivo tras la primera instalación de IPCop, y puede ser activado (y desactivado) mediante la página Servicios > Proxy.

Nota

La página de registros del proxy *sólo* mostrará registros si ha activado el registro en la página Servicios > Proxy.

Debido a la gran cantidad de información que ha de ser procesada, la página Proxy Web puede tomar un tiempo en mostrarse tras seleccionarla o tras pulsar Actualizar.

Hay varios controles en esta página, además de los controles básicos Mes, Día, << (Día anterior), >> (Día siguiente), Actualizar y Exportar descritos al principio de esta Sección:

- El menú desplegable IP de origen: le permite ver la actividad del proxy relativa a una única dirección IP de la red local o la actividad relativa a TODAS las máquinas que han usado el proxy.
- La caja Filtro ignorar: le permite escribir una expresión regular de texto para definir qué tipos de archivos deben ser omitidos del registro del proxy web. La cadena por defecto oculta las imágenes (`.gif .jpeg .jpg` y `.png`), las hojas de estilos (`.css`) y archivos JavaScript (`.js`).
- La casilla Activar filtro ignorar: le permite controlar si el Filtro ignorar: está activo o no.

- El botón Restaurar por defecto le permite devolver los controles anteriores y los filtros a los por defecto.

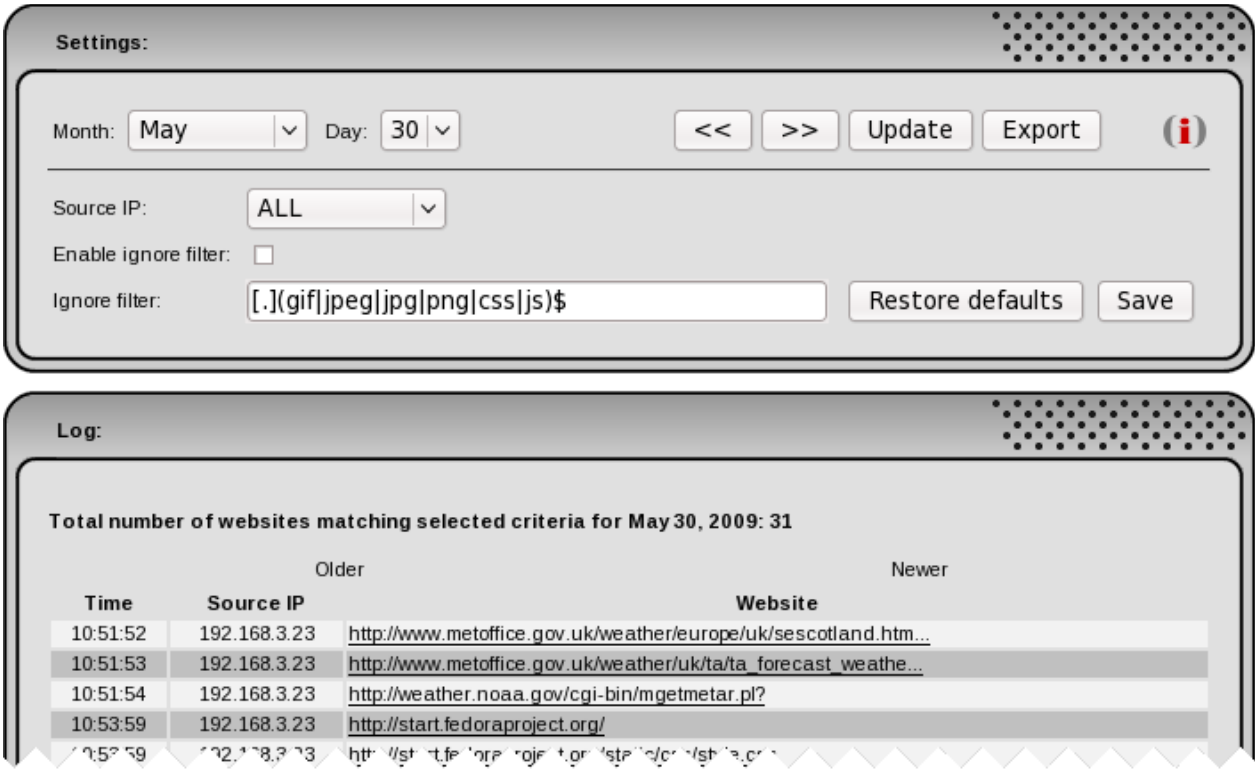
En esta página, la información de registro que aparece en la sección Registro: de la ventana consiste en:

- La Hora en la que el archivo fue solicitado y cacheado.
- La dirección IP de origen del sistema local que pidió el archivo.
- El Sitio web - o más concretamente, la URL de cada archivo solicitado y cacheado.

Nota

Las entradas URL en Sitio web son también enlaces a las páginas o archivos referenciados.

Figura 2.78. Salida de Registros del Proxy



2.8.4. Página de registros del cortafuegos

Esta página muestra los paquetes de datos que han sido bloqueados por el cortafuegos de IPCop.

Nota

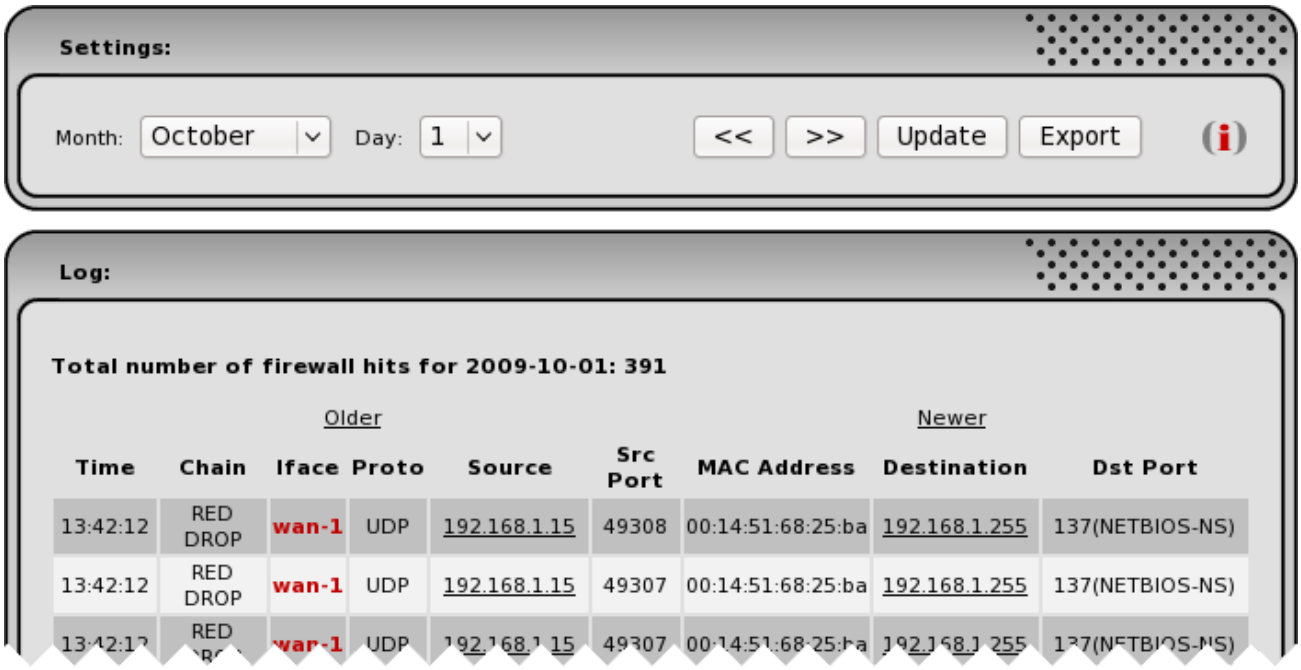
No todos los paquetes denegados son intentos hostiles de crackers para conseguir acceso a su máquina. Normalmente, los bloqueos de paquetes se dan por varias razones inofensivas y pueden ser ignorados tranquilamente. Entre ellas se pueden encontrar los intentos de conexión al puerto "ident/auth" (113), que por defecto son bloqueados por IPCop.

Los controles en esta página son los botones básicos Mes, Día, << (Día anterior), >> (Día siguiente), Actualizar y Exportar que se han descrito en detalle al principio de esta sección.

La sección Registro: de esta página contiene una entrada para cada paquete que fue "descartado" por el cortafuegos. Incluye la hora del evento, las direcciones IP y puertos de origen y destino del paquete descartado, el protocolo empleado por ese paquete y la cadena e interfaz de IPCop que han intervenido.

Puede obtener información sobre las direcciones IP listadas pinchando en cada dirección IP. IPCop realiza una búsqueda DNS y devuelve la información disponible acerca de su registro y propiedad.

Figura 2.79. Salida de registros del cortafuegos



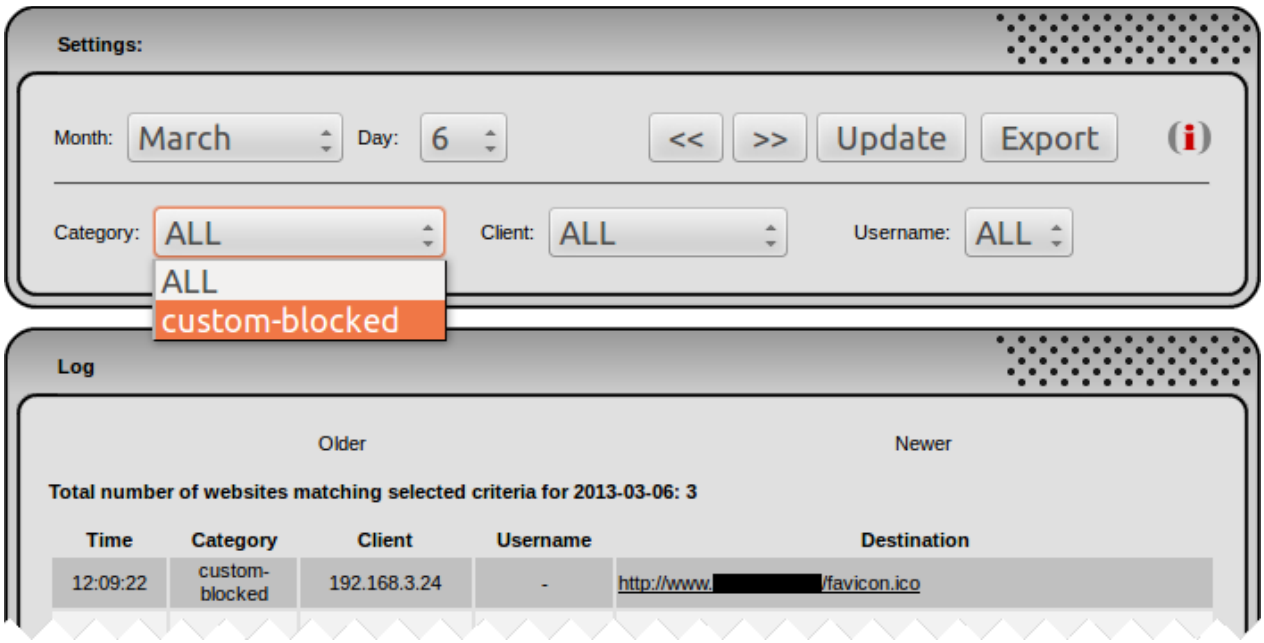
2.8.5. Registros de URL Filter

Esta página muestra las peticiones que han sido bloqueadas por el filtro `squidguard`.

Hay tres menús desplegables además de los habituales controles Mes, Día, << (Día anterior), >> (Día siguiente), Actualizar y Exportar que se han descrito en detalle al principio de esta sección, y que le permiten filtrar los resultados aún más:

- El menú desplegable Categoría: le permite ver TODAS las peticiones bloqueadas o sólo las de una categoría en particular.
- El menú desplegable Cliente: le permite filtrar los resultados de un cliente en particular o mostrar TODOS ellos.
- El menú desplegable Usuario: le permite ver TODAS las peticiones de todos los usuarios, o sólo los de un usuario en particular.

Recuerde pulsar el botón Actualizar tras realizar una selección para refrescar el contenido.



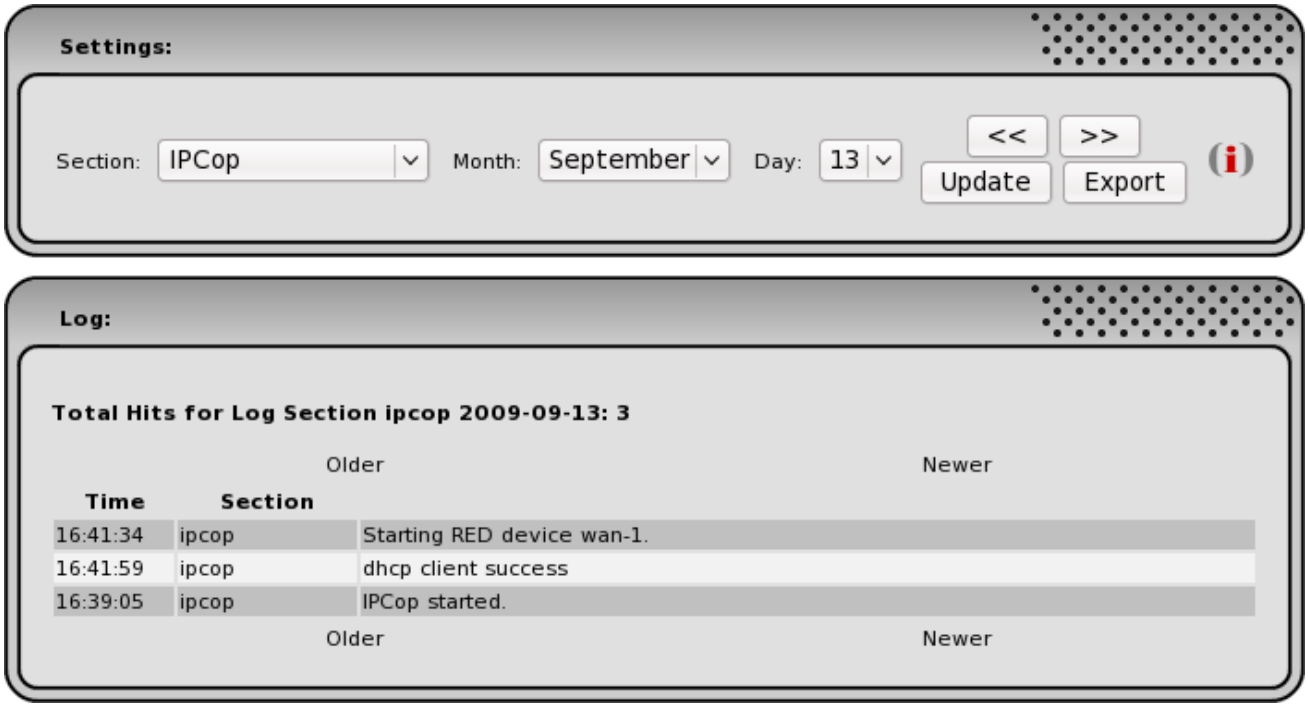
2.8.6. Página de registros del Sistema

Esta página le permite ver los registros del sistema y otros varios. (Consulte el principio de esta sección sobre cómo usar los controles Mes, Día, << (Día anterior), >> (Día siguiente) y Actualizar). Hay unas doce categorías diferentes, seleccionables mediante la lista desplegable Sección:

- IPCop (por defecto) - eventos generales de IPCop, como el guardado de un perfil PPP y conexiones ("`PPP se ha levantado en ppp0`") y desconexiones ("`PPP se ha caído en ppp0`") de los enlaces por módem anaógico.
- Cron - muestra un registro de la actividad del demonio fcron.
- Servidor DHCP - muestra un registro de la actividad de la función de servidor DHCP de IPCop.
- DNS - muestra un registro de la actividad de dnsmasq, la utilidad de servidor de nombres de dominio.
- IPSec - es un registro de la actividad de IPsec - un módulo de software usado por IPCop.
- Núcleo - es un registro de la actividad del núcleo del servidor IPCop.
- Accesos/Salidas - muestra un registro de los usuarios que han accedido y salido del servidor IPCop. Esto incluye tanto los accesos locales como los accesos desde una red mediante la interfaz SSH.
- NTP - muestra un registro de la actividad del servidor ntpd.
- OpenVPN - es un registro de la actividad de OpenVPN - un módulo de software usado por IPCop.
- Proxy - muestra un registro de la actividad de squid, el proxy caché utilizado por IPCop.

- ROJA - el tráfico enviado a través de la interfaz que proporciona la interfaz PPP a IPCop. Esto incluye las cadenas de datos enviadas y recibidas a/desde un módem. Esto puede ser un recurso muy útil para resolver situaciones de “fallo al conectar”.
- SSH - muestra un registro de los usuarios que han accedido o salido del servidor IPCop desde una red mediante la interfaz SSH.
- Recuento de tráfico - muestra un registro de la actividad de los demonios de monitorización, si están activados.
- Resultado de actualizaciones - es un registro de los resultados de todas las actualizaciones aplicadas al software de IPCop mediante la ventana Sistema > Actualizaciones.

Figura 2.80. Salida de Registros del sistema



2.9. Personalización por el usuario.

Existen varios archivos y scripts que permiten al Administrador configurar IPCop para adaptarlo a su entorno particular.

Esta sección explica qué hacen los archivos y scripts y dónde encontrarlos.

No cubre los add-ons creados por la Comunidad.

Necesitará tener acceso a una terminal como 'root' para poder editar archivos con el editor **vi**.

2.9.1. rc.event.local

El script shell `/etc/rc.d/rc.event.local` reemplaza al archivo `/etc/rc.d/rc.local` de versiones anteriores, y amplía su funcionalidad. Ahora es llamado cuando IPCop arranca, se apaga, cuando alguna interfaz de red (excepto ROJA) se inician o se paran, o cuando la interfaz ROJA se levanta o se tumba. Puede contener sus propios comandos para que sean ejecutados al ocurrir alguno de estos eventos concretos.

Por ejemplo, el script es llamado así al arrancar:

`/etc/rc.d/rc.event.local system up`

El primer parámetro es un evento: system, network, red

El segundo parámetro es un valor: up, down

Busque en este archivo un ejemplo de cómo añadir sus propios comandos. Por ejemplo, para configurar un módem interno en el inicio, podría hacer lo siguiente:

```
if [ ${1} == "system" -a ${2} == "up" ]; then
    echo "Configurando módem..."
    setserial /dev/ttyS2 uart 16550A irq 12 port 0x2400
fi
```

(La irq y número de puerto son sólo ejemplos, y pueden variar entre diferentes sistemas).

O si quiere activar el apagado de una pantalla conectada a IPCop, que actúe como salvapantallas y evite el desgaste poniendo en negro la pantalla tras un período de inactividad, puede añadir lo siguiente:

```
if [ ${1} == "system" -a ${2} == "up" ]; then
    echo -e "Apagando pantalla ... \033[9;1]"
fi
```

El archivo `rc.event.local` no se sobreescribirá por *Actualizaciones Oficiales*, y está incluido en el conjunto de archivos salvados cuando se hace una copia de seguridad del sistema.

2.9.2. exclude.user

El archivo `/var/ipcop/backup/exclude.user` puede ser editado por Administradores para **excluir** archivos de la copia de seguridad del sistema.

Este archivo no se sobreescribirá por *Actualizaciones Oficiales*, y está incluido en el conjunto de archivos salvados cuando se hace una copia de seguridad del sistema.

Eche un vistazo a `/var/ipcop/backup/exclude.system` para ver el formato.

2.9.3. include.user

El archivo `/var/ipcop/backup/include.user` puede ser editado por Administradores para **incluir** archivos en la copia de seguridad del sistema.

Este archivo no se sobreescribirá por *Actualizaciones Oficiales*, y está incluido en el conjunto de archivos salvados cuando se hace una copia de seguridad del sistema.

Eche un vistazo a `/var/ipcop/backup/include.system` para ver el formato.

2.9.4. Personalización de cadenas de IPTables

Hay cadenas específicas que los usuarios de IPCop pueden emplear para añadir sus propias reglas. Sus nombres: `CUSTOMINPUT`, `CUSTOMFORWARD`, `CUSTOMOUTPUT`, `CUSTOMPREROUTING` y `CUSTOMPOSTROUTING`

Los Administradores pueden añadir sus propias reglas al cortafuegos en el archivo `/etc/rc.d/rc.firewall.local`

2.9.5. rc.firewall.local

Este script shell permite a los Administradores crear sus propios cambios a las reglas del cortafuegos. Eche un vistazo al archivo `/etc/rc.d/rc.firewall.local`

Es llamado por `/etc/rc.d/rc.firewall`, y para utilizarlo manualmente, su uso es:

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

Este archivo no se sobreescribirá por *Actualizaciones Oficiales*, y está incluido en el conjunto de archivos salvados cuando se hace una copia de seguridad del sistema.

2.9.6. dnsmasq.local

El archivo `/var/ipcop/dhcp/dnsmasq.local` permite a los Administradores añadir sus propias opciiones al servidor DHCP.

Visite el manual de dnsmasq para más información.

Por ejemplo, para dar una dirección fija a una máquina con dos interfaces de red (p.e. un portátil con interfaz cableada e inalámbrica) añada esta línea:

```
dhcp-
host=XX:XX:XX:XX:XX:XX,YY:YY:YY:YY:YY:YY,192.168.3.200
```

O para enlazar un archivo que contenga una lista de dominios que desea bloquear, como un conjunto de sitios de publicidad, añada esta línea a `dnsmasq.local`:

```
conf-file=/path-to-your/blocklist
```

Esta lista de bloqueos debe contener una lista de direcciones en el formato siguiente:

```
address=/domain-name/127.0.0.1
address=/another-domain-name/127.0.0.1
...
```

Reinicie el servidor DHCP mediante la interfaz web o **restartdhcp** tras modificar `dnsmasq.local` para que sus cambios se propaguen por la red.

Este archivo no se sobreescribirá por *Actualizaciones Oficiales*, y está incluido en el conjunto de archivos salvados cuando se hace una copia de seguridad del sistema.

.9.7. setreservedports.pl

Se proporciona el script de línea de comandos **setreservedports.pl** para permitir a los Administradores cambiar el puerto seguro o el puerto de acceso SSHd.

Para cambiar el puerto https, utilice la opción **--gui** :

```
$ /usr/local/bin/setreservedports.pl --gui 5445
```

Aunque aquí se sugiere el uso del puerto 5445 como puerto alternativo, se permite cualquier puerto entre 1 y 65535, siempre que no lo utilice otro servicio.

Para cambiar el puerto ssh, utilice la opción **--ssh** :

```
$ /usr/local/bin/setreservedports.pl --ssh 5022
```

2.10. Servidor Proxy Web

Esta sección describe más en profundidad los métodos de *Autenticación de usuario* disponibles en las Opciones Avanzadas del proxy web.

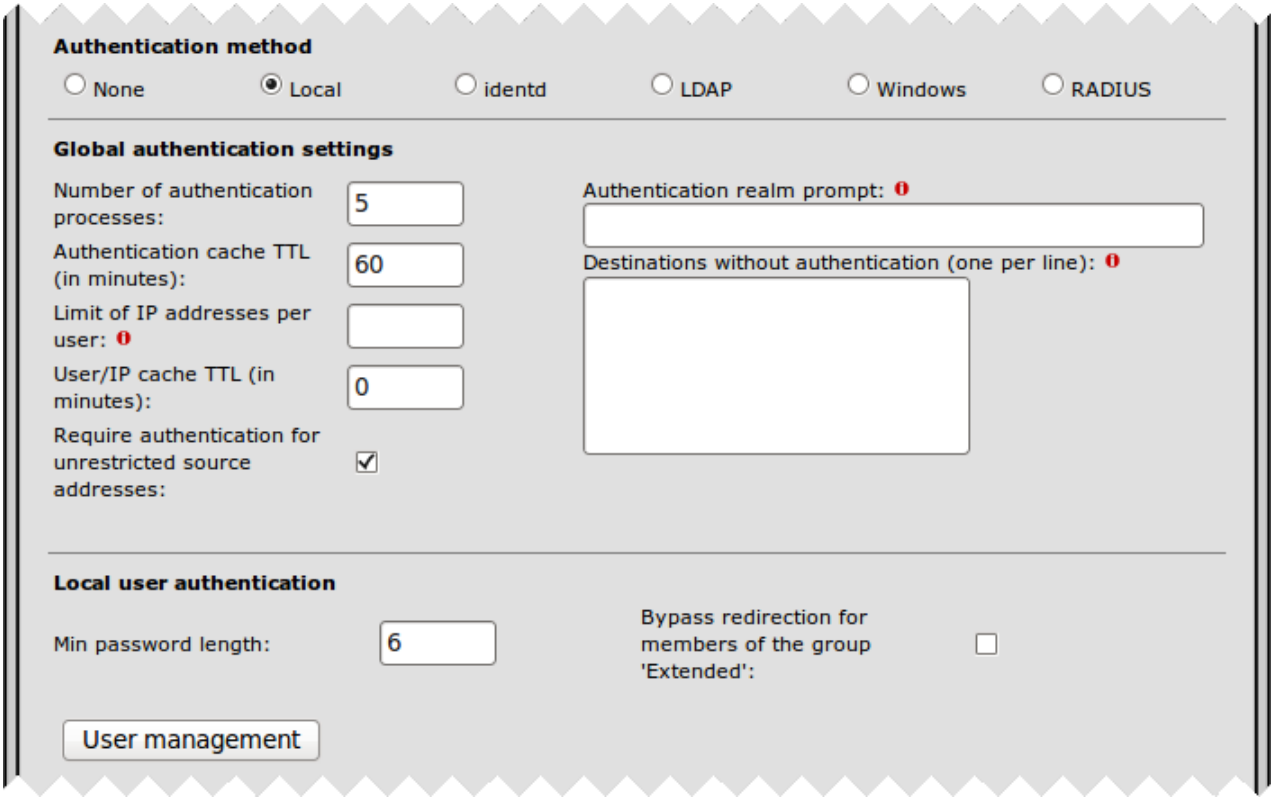
Para instituciones educacionales, las Opciones Avanzadas también proporcionan las *Extensiones de Aula*, una interfaz de administración para el personal docente.

- Autenticación Proxy Local
- Autenticación identd
- Autenticación LDAP
- Autenticación Windows
- Autenticación RADIUS
- Extensiones de Aula

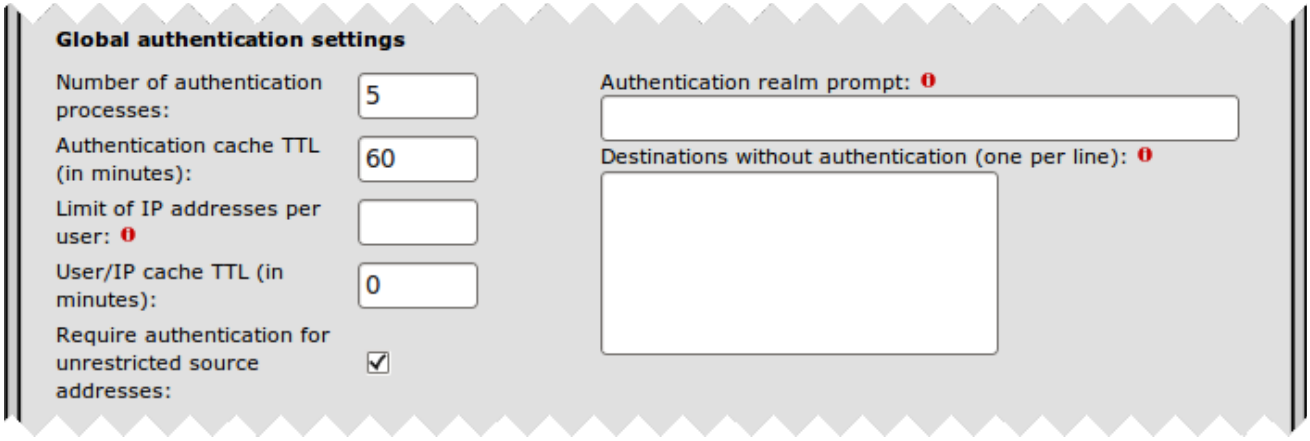
2.10.1. Autenticación Proxy Local

La autenticación de usuario local es la mejor solución para entornos SOHO. Los usuarios necesitan autenticarse cuando acceden a sitios web introduciendo un nombre de usuario y una contraseña. La gestión de usuarios reside en el servidor proxy de IPCop. Los usuarios están categorizados en tres grupos: *Extendido*, *Estándar* and *Desactivado*.

Este método de autenticación le permite gestionar las cuentas de usuario localmente sin la necesidad de servidores externos de auntenticación.



2.10.1.1. Ajustes de autenticación globales



Número de procesos de autenticación. El número de procesos en segundo plano a la escucha de peticiones. El valor por defecto es 5 y debería ser incrementado si la autenticación toma demasiado tiempo o la autenticación integrada de Windows pasa a autenticación explícita.

TTL de la caché de autenticación. El tiempo en minutos durante el cual las credenciales se mantendrán en caché para cada sesión. Si este tiempo expira, el usuario tiene que volver a introducir las credenciales para esa sesión. Por defecto es de 60 minutos, el mínimo es de 1 minuto. El TTL se reinicia cada vez que el usuario envía una petición al servidor Proxy durante una sesión.

Nota

Si el usuario abre una nueva sesión, las credenciales siempre tienen que ser introducidas, incluso si el TTL no ha expirado para otra sesión.

Límite de direcciones IP por usuario (opcional). Número de direcciones IP de origen desde las que un usuario puede estar autenticado a la vez. La dirección IP se liberará tras el tiempo establecido en *TTL de la caché de Usuario/IP.*

Nota

Esto no tiene efecto si se está usando autenticación Local y el usuario es miembro del grupo *Extendido*.

TTL de la caché de Usuario/IP. Tiempo en minutos durante el cual se mantendrán en caché las relaciones entre cada usuario y la dirección IP empleada. El valor por defecto es 0 (desactivado).

Un valor mayor de 0 sólo tiene sentido cuando se emplea un límite de direcciones IP concurrentes por usuario.

Requerir autenticación para direcciones de origen no restringidas. Por defecto se requiere autenticación incluso para las direcciones IP no restringidas. Si no quiere requerir autenticación a esas direcciones, desmarque esta casilla.

Texto del diálogo de autenticación. Este texto se mostrará en el diálogo de autenticación. Por defecto es “Servidor Proxy Avanzado de IPCop”.

Destinos sin autenticación. Esto le permite definir una lista de destinos que pueden ser accedidos sin autenticación.

Nota

Cualquier dominio listado aquí son dominios de destino DNS y no dominios de origen Windows NT.

Ejemplos:

Dominios completos y subdominios

```
*.ejemplo.net
*.google.com
```

Hosts únicos

```
www.ejemplo.net
www.google.com
```

Direcciones IP

```
81.169.145.75
74.125.39.103
```

URLs

```
www.ejemplo.net/download
www.google.com/images
```

Nota

Puede introducir todos estos tipos de destino en cualquier orden.

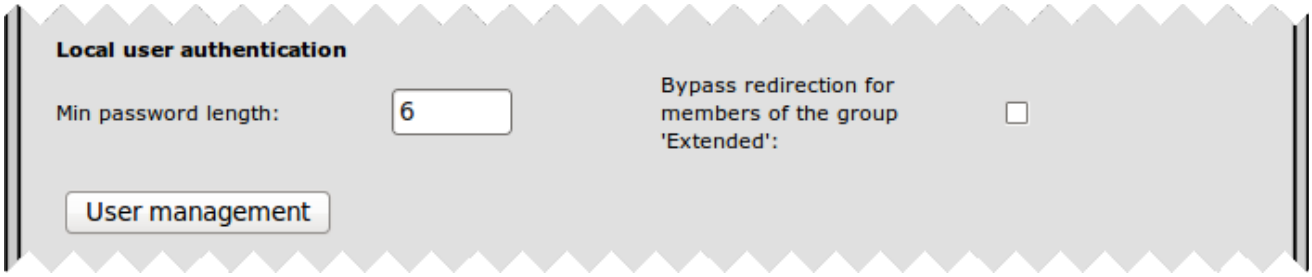
Ejemplo para Windows Update.

Para permitir acceder a Windows Update sin autenticación añada estos destinos a la lista:

```
*.download.microsoft.com
*.windowsupdate.com
windowsupdate.microsoft.com
```

2.10.1.2. Autenticación de usuario local

La gestión integrada de usuarios puede ser ejecutada desde la página principal de ajustes.



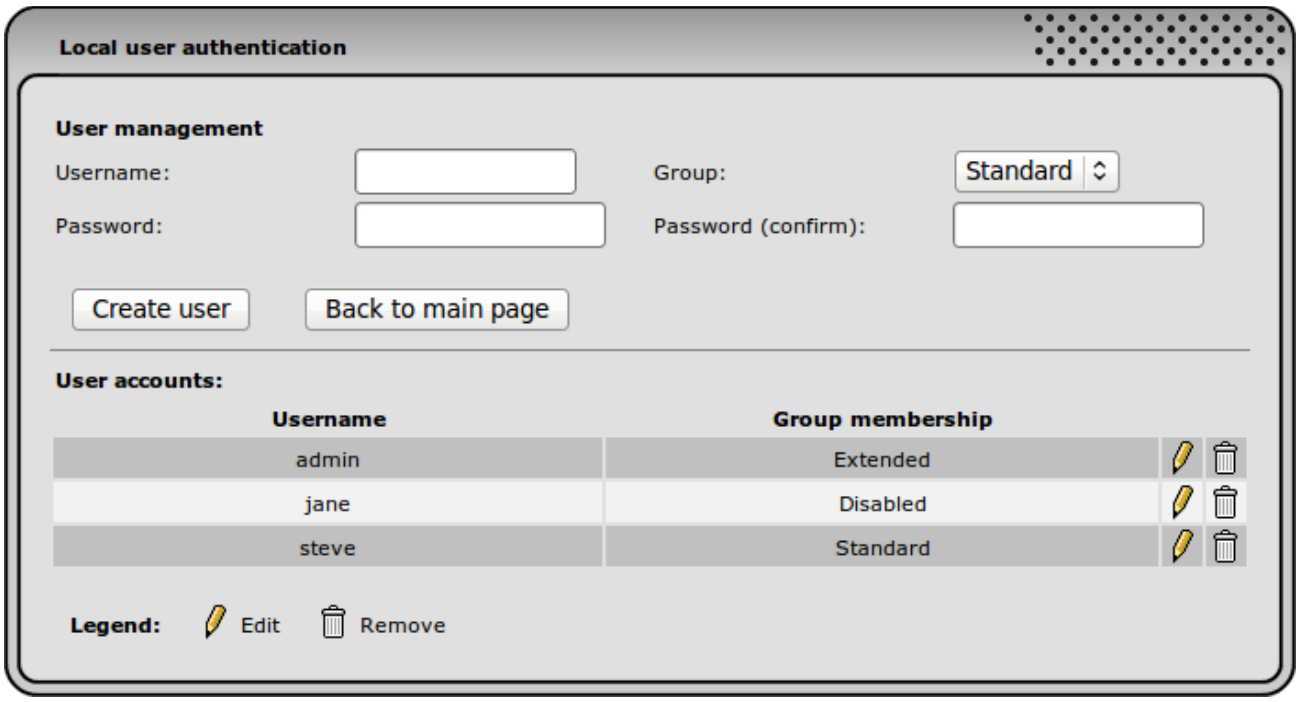
Longitud mínima de contraseña. Introduzca la longitud mínima requerida para las contraseñas. Por defecto es de 6 caracteres alfanuméricos.

Saltar redirección para miembros del grupo extendido. Si hay instalado cualquier redirector (como el 'add on' URL filter), todos los miembros del grupo *Extendido* se saltarán este redirector.

Gestión de usuarios. Este botón abre el gestor de usuarios locales.

2.10.1.3. Gestor de usuarios locales

El gestor de usuarios es la interfaz para crear, editar y borrar cuentas de usuario.



En la página de gestión de usuarios, se listan todas las cuentas disponibles en orden alfabético.

Definición de grupos. Puede seleccionar entre tres grupos diferentes:

Estándar

El grupo por defecto para todos los usuarios. Todas las restricciones establecidas se aplican a este grupo.

Extendido

Use este grupo para usuarios sin restricciones. Los miembros de este grupo se saltarán cualquier restricción de tiempo y de filtrado.

Desactivado

Los miembros de este grupo están bloqueados. Esto puede ser útil si quiere desactivar una cuenta temporalmente sin perder la contraseña.

Requerimientos de reinicio del servicio de Proxy. Los siguientes cambios en las cuentas de usuario requerirán un reinicio del servicio de Proxy:

- Se ha añadido una nueva cuenta de usuario y el usuario no es miembro del grupo *Estándar*.
- La membresía de grupo de un usuario se ha cambiado.

Los siguientes cambios en las cuentas de usuario *no* requieren reiniciar el servicio de Proxy:

- Se ha añadido una nueva cuenta de usuario y el usuario es miembro del grupo *Estándar*.
- Se ha cambiado la contraseña de un usuario.
- Se ha borrado una cuenta de usuario.

2.10.1.4. Crear cuentas de usuario

Nombre de usuario. Introduzca el nombre de usuario. Si es posible, el nombre sólo debería contener caracteres alfanuméricos.

Grupo. Seleccione el grupo al que pertenecerá este usuario.

Contraseña. Introduzca la contraseña para la nueva cuenta.

Contraseña (confirmar). Confirme la contraseña introducida anteriormente.

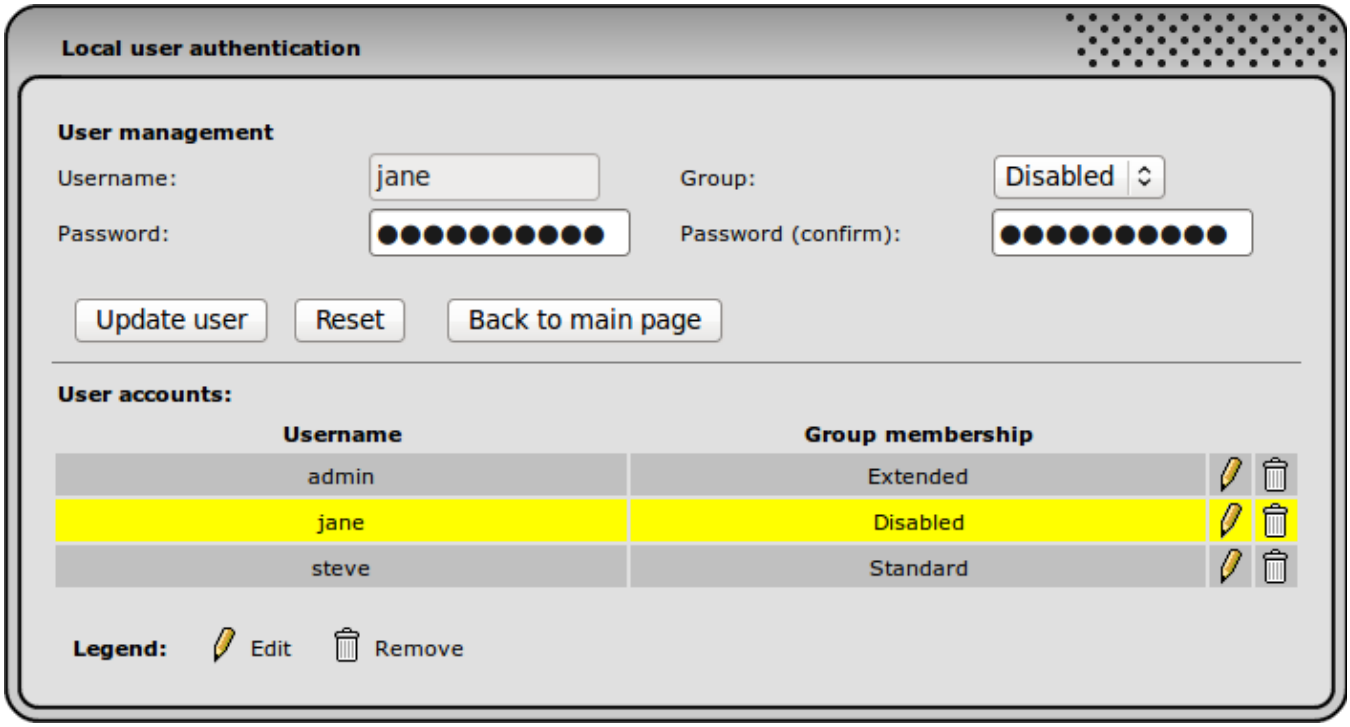
Crear usuario. Este botón crea una nueva cuenta de usuario. Si el nombre de usuario ya existe, la cuenta de este nombre de usuario se actualizará con el nuevo grupo y contraseña.

Volver a la página principal. Este botón cierra el gestor de usuarios y vuelve a la página principal.

2.10.1.5. Editar cuentas de usuario

Se puede editar una cuenta de usuario pinchando en el icono del *lápiz amarillo*. Cuando se edita una cuenta de usuario, sólo se puede cambiar el grupo o la contraseña.

Cuando se está editando una cuenta, la entrada referida se marca con una barra amarilla.



Para guardar los cambios, use el botón Actualizar usuario.

Nota

El nombre de usuario no se puede modificar. Este campo es de sólo lectura. Si necesita renombrar un usuario, borre el usuario y cree una nueva cuenta.

2.10.1.6. Borrar cuentas de usuario

Se puede borrar una cuenta de usuario pinchando en el icono de la *papelera*. La cuenta se borrará inmediatamente.

2.10.1.7. Gestión de contraseñas por el cliente

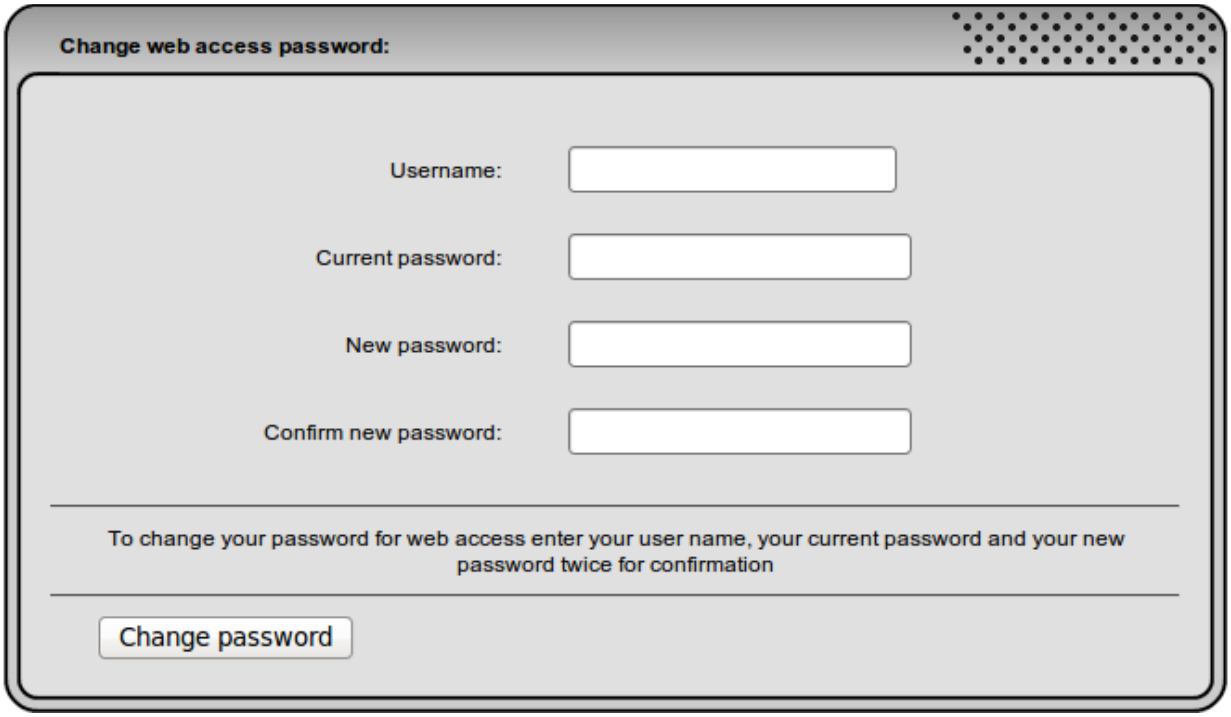
Los usuarios pueden cambiar sus contraseñas si lo necesitan. Se accede a la interfaz introduciendo esta URL:

http://192.168.1.1:81/cgi-bin/chpasswd.cgi

Nota

Reemplace *192.168.1.1* con la dirección IP VERDE de su IPCop.

El diálogo de la página web requiere el usuario, la contraseña actual y la contraseña nueva (dos veces para confirmar).

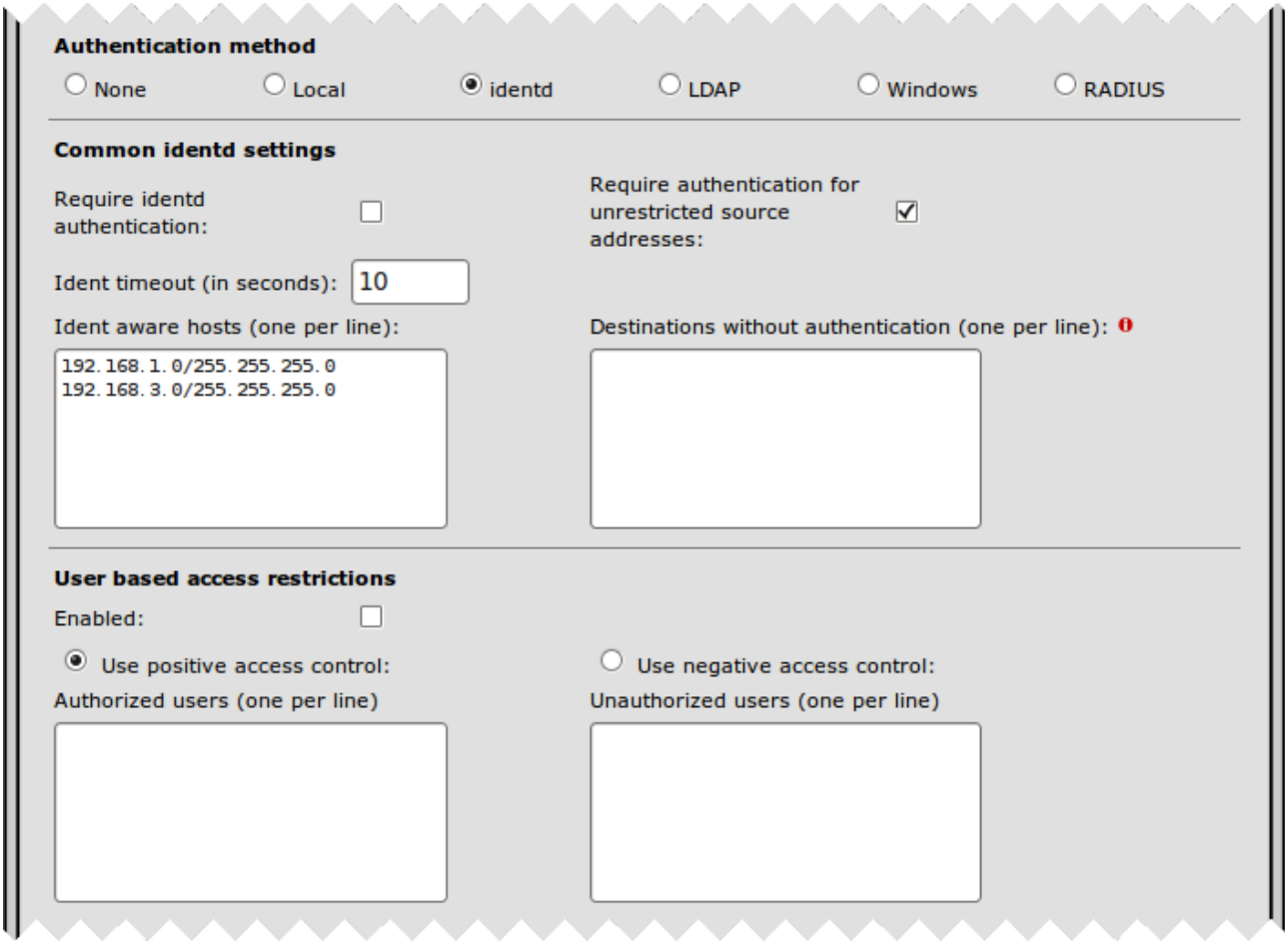


2.10.2. Autenticación identd

Este método de autenticación es el más adecuado en entornos donde:

- La autenticación tiene que ser un proceso “oculto” sin introducir nombre de usuario y contraseña.
- El servicio de proxy debe operar en modo transparente.
- Los nombres de usuario sólo se utilizarán para registro y no para autenticación.

El método de autenticación identd requiere un servicio o demonio **identd** corriendo en el cliente. A diferencia de otros métodos de autenticación, identd no tiene la sección “Ajustes de autenticación globales”.



Además de la autenticación, puede definir listas positivas o negativas de control de acceso basadas en usuarios.

2.10.2.1. Prerequisitos del cliente

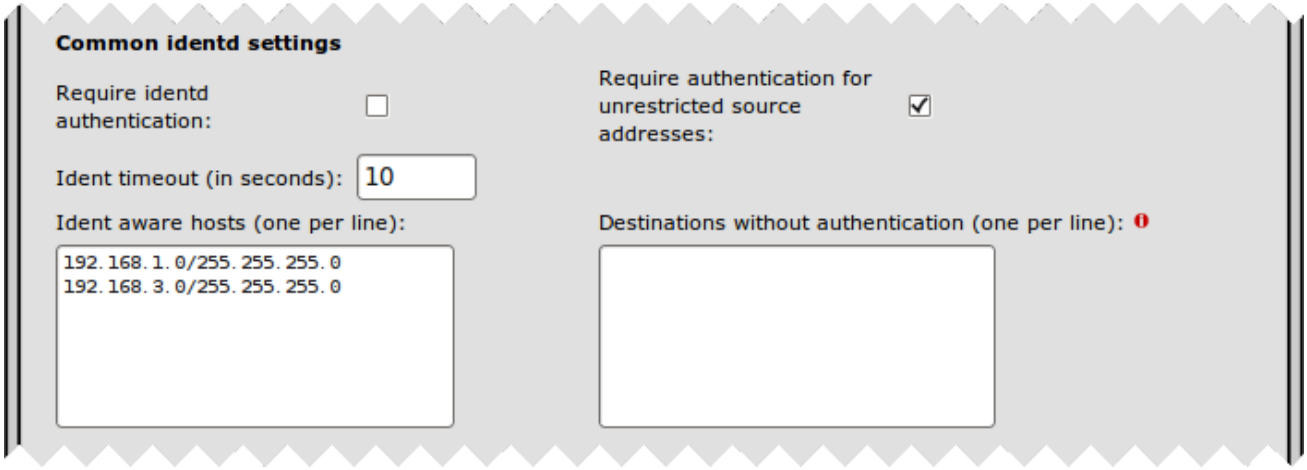
La mayoría de clientes basados en Linux ya tienen un demonio identd (**identd**) instalado por defecto.

Para clientes Windows, hay varias implementaciones libres de **identd** disponibles. Esta funciona en Windows XP y Vista: rndware's Windows Ident Server

Nota

El puerto 113 (TCP) tiene que estar abierto en los cortafuegos de los clientes.

2.10.2.2. Ajustes comunes de identd



Requerir autenticación identd. Por defecto, la autenticación **identd** no será obligatoria. Esta configuración puede ser útil para propósitos de registro. Si quiere usar **identd** para autenticación forzada, esta opción tiene que activarse. El acceso a los clientes que no se autentiquen usando **identd** será denegado.

Nota

El proxy no puede correr en modo transparente cuando se utilice autenticación **identd**.

Requerir autenticación para direcciones de origen no restringidas. Si "Requerir autenticación identd" está activado, también se requerirá autenticación para las direcciones IP no restringidas. Si no quiere requerir autenticación para direcciones IP no restringidas, desmarque esta casilla.

Tiempo de espera ident. Tiempo máximo en segundos que el proxy esperará a que las búsquedas ident se completen.

Hosts con ident activo. Esto habilita las búsquedas ident para las direcciones de clientes listadas. Las direcciones de clientes que no estén listadas aquí no recibirán peticiones ident.

Nota

Los clientes no listados obtendrán acceso sin autenticación, incluso si la opción "Requerir autenticación identd" está activada.

Destinos sin autenticación (opcional). Esto le permite definir una lista de destinos que pueden ser accedidos sin autenticación.

Nota

Cualquier dominio listado aquí son dominios de destino DNS y no dominios de origen Windows NT.

Ejemplos:

Dominios completos y subdominios

```
*.ejemplo.net
*.google.com
```

Hosts únicos

```
www.ejemplo.net
www.google.com
```

Direcciones IP

```
81.169.145.75
74.125.39.103
```

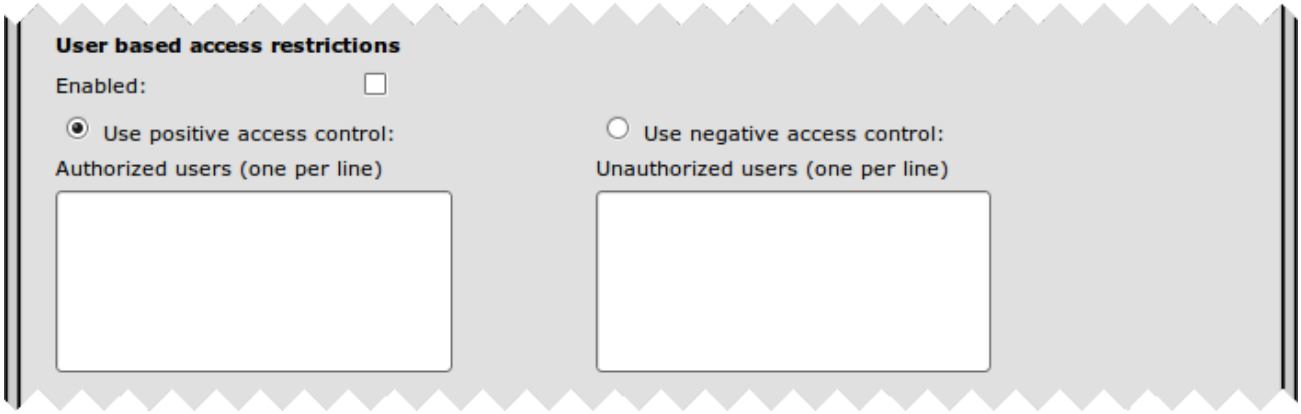
URLs

```
www.ejemplo.net/download
www.google.com/images
```

Nota

Puede introducir todos estos tipos de destino en cualquier orden.

2.10.2.3. Restricciones basadas en usuario



Activado. Activa las listas de control de acceso para usuarios autorizados o denegados.

Utilizar control de acceso positivo / Usuarios autorizados. Los usuarios listados aquí tendrán acceso web. Para todos los demás usuarios, el acceso será denegado.

Utilizar control de acceso negativo / Usuarios denegados. Los usuarios listados aquí tendrán el acceso web bloqueado. Para todos los demás usuarios, el acceso estará permitido.

2.10.3. Autenticación LDAP

Este método de autenticación es el más adecuado en entornos de red medios y grandes. Los usuarios se tendrán que autenticar cuando accedan a sitios web entrando un nombre de usuario y contraseña válidos. Las credenciales son verificadas contra un servidor externo usando el Protocolo Ligero de Acceso a Directorios (LDAP).

La autenticación LDAP es útil si ya tiene un servicio de directorio en su red y no quiere mantener cuentas de usuario y contraseñas adicionales para el acceso web.

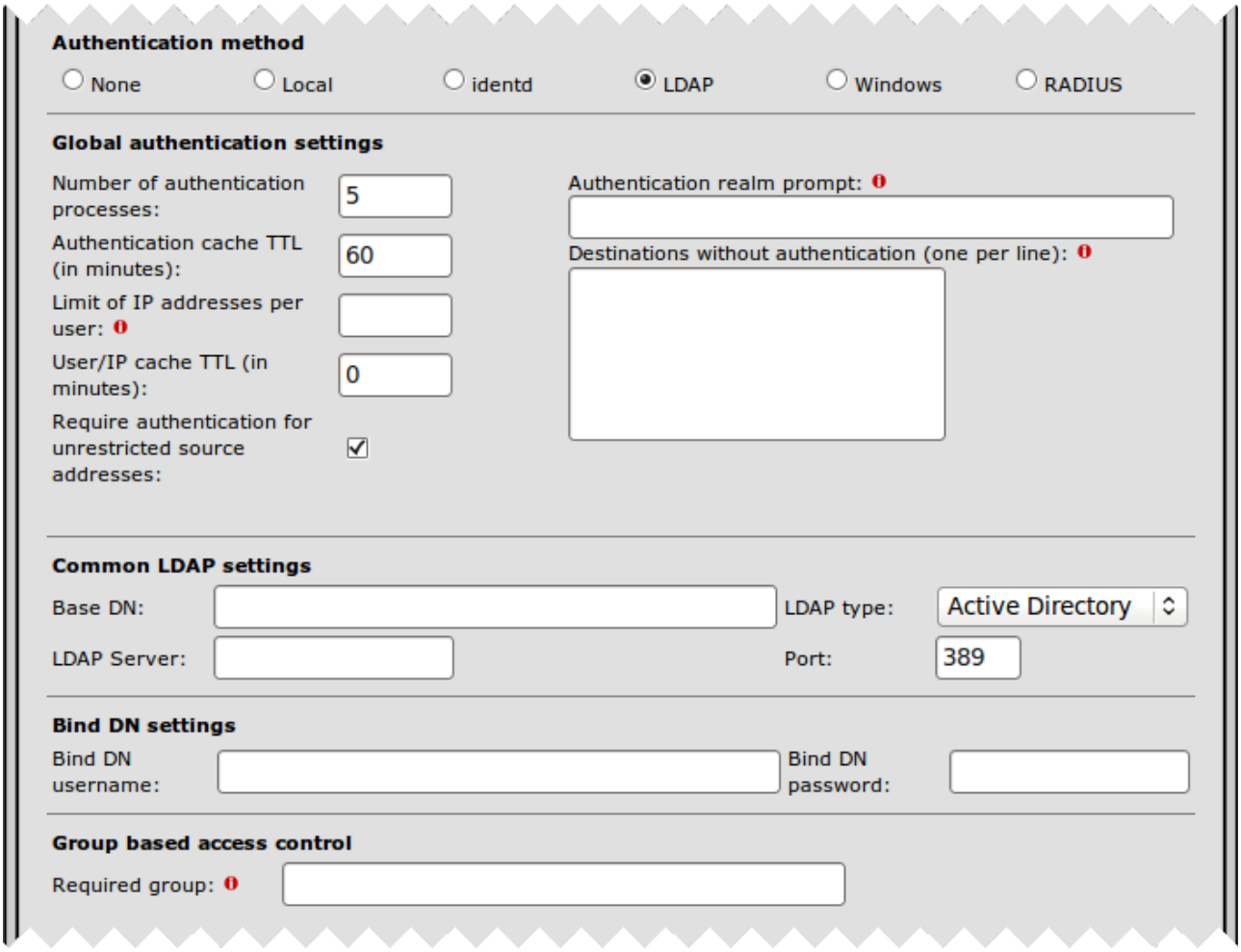
El Proxy Avanzado trabaja con estos tipos de servidores LDAP:

- Directorio Activo (Windows 2000, 2003 y 2008 Server)
- Novell eDirectory (NetWare 5.x y NetWare 6)
- LDAP Versión 2 and 3 (OpenLDAP)

Como opción, se puede requerir la membresía a un cierto grupo.

Nota

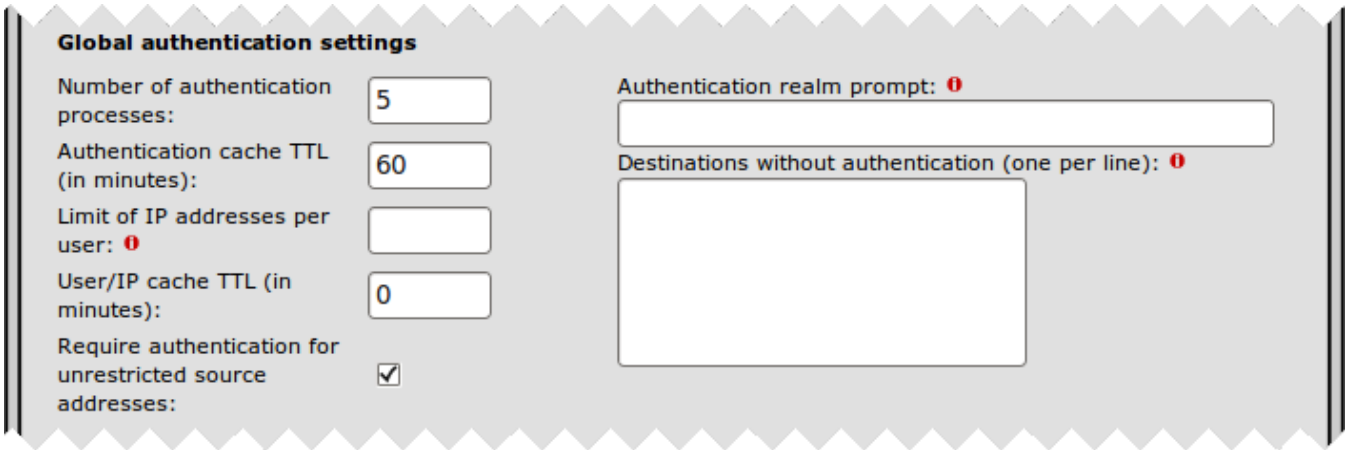
El protocolo LDAPS (LDAP seguro) no está soportado por el Proxy Avanzado.



Si no está seguro acerca de su estructura de directorio interna, puede examinar sus servidores LDAP usando la herramienta de línea de comandos *ldapsearch*.

Los clientes Windows pueden usar para esto el navegador LDAP Softerra, gratuito y fácil de usar: http://www.ldapbrowser.com

2.10.3.1. Ajustes de autenticación globales



Número de procesos de autenticación. El número de procesos en segundo plano a la escucha de peticiones. El valor por defecto es 5 y debería ser incrementado si la autenticación toma demasiado tiempo o la autenticación integrada de Windows pasa a autenticación explícita.

TTL de la caché de autenticación. El tiempo en minutos durante el cual las credenciales se mantendrán en caché para cada sesión. Si este tiempo expira, el usuario tiene que volver a introducir las credenciales para esa sesión. Por defecto es de 60 minutos, el mínimo es de 1 minuto. El TTL se reinicia cada vez que el usuario envía una petición al servidor Proxy durante una sesión.

Nota

Si el usuario abre una nueva sesión, las credenciales siempre tienen que ser introducidas, incluso si el TTL no ha expirado para otra sesión.

Límite de direcciones IP por usuario (opcional). Número de direcciones IP de origen desde las que un usuario puede estar autenticado a la vez. La dirección IP se liberará tras el tiempo establecido en *TTL de la caché de Usuario/IP*.

Nota

Esto no tiene efecto si se está usando autenticación Local y el usuario es miembro del grupo *Extendido*.

TTL de la caché de Usuario/IP. Tiempo en minutos durante el cual se mantendrán en caché las relaciones entre cada usuario y la dirección IP empleada. El valor por defecto es 0 (desactivado).

Un valor mayor de 0 sólo tiene sentido cuando se emplea un límite de direcciones IP concurrentes por usuario.

Requerir autenticación para direcciones de origen no restringidas. Por defecto se requiere autenticación incluso para las direcciones IP no restringidas. Si no quiere requerir autenticación a esas direcciones, desmarque esta casilla.

Texto del diálogo de autenticación. Este texto se mostrará en el diálogo de autenticación. Por defecto es “Servidor Proxy Avanzado de IPCop”.

Destinos sin autenticación. Esto le permite definir una lista de destinos que pueden ser accedidos sin autenticación.

Nota

Cualquier dominio listado aquí son dominios de destino DNS y no dominios de origen Windows NT.

Ejemplos:

Dominios completos y subdominios

```
*.ejemplo.net
*.google.com
```

Hosts únicos

```
www.ejemplo.net
www.google.com
```

IP addresses

```
81.169.145.75
74.125.39.103
```

URLs

```
www.ejemplo.net/download
www.google.com/images
```

Nota

Puede introducir todos estos tipos de destino en cualquier orden.

Ejemplo para Windows Update.

Para permitir acceder a Windows Update sin autenticación añada estos destinos a la lista:

```
*.download.microsoft.com
*.windowsupdate.com
windowsupdate.microsoft.com
```

2.10.3.2. Ajustes comunes LDAP

Base de DN (Nombre de Dominio). Esta es la base donde comienza la búsqueda LDAP. Todas las Unidades de Organización (OUs) subsiguientes serán incluidas.

Consulte en la documentación de su LDAP el formato requerido de la base de DN.

Ejemplo de base de DN para Directorio Activo:

```
cn=usuarios,dc=ads,dc=local
```

Esto buscará usuarios en el grupo *usuarios* en el dominio *ads.local*

Ejemplo de base de DN para eDirectory:

```
ou=usuarios,o=acme
```

Esto buscará usuarios en la Unidad de Organización *usuarios* (y por debajo) en la Organización *acme*

Nota

Si la base de DN contiene espacios, debe “preceder” estos espacios con una barra invertida.

Ejemplo para una base de DN con espacios:

```
cn=usuarios\ internet,dc=ads,dc=local
```

Tipo de LDAP. Puede seleccionar entre diferentes tipos de implementaciones de LDAP:

- Directorio Activo (ADS)
- Novell eDirectory (NDS)
- LDAP v2 y v3

Servidor LDAP. Introduzca la dirección IP de su servidor LDAP.

Puerto. Introduzca el puerto en el que su servidor LDAP está escuchando peticiones. Por defecto es el 389.

Nota

El protocolo LDAPS (LDAP Seguro, puerto 636) no está soportado por el Proxy Avanzado.

2.10.3.3. Ajustes de Bind DN

Nombre de usuario Bind DN. Introduzca el nombre distinguido completo de un usuario Bind DN.

Nota

Se requiere un usuario Bind DN para Directorio Activo y eDirectory.

Al usuario Bind DN se le debe permitir navegar por el directorio y leer todos los atributos de usuario.

Si el nombre de usuario Bind DN contiene espacios, debe "preceder" estos espacios con una barra invertida.

Contraseña Bind DN. Introduzca la contraseña del usuario Bind DN.

2.10.3.4. Control de acceso basado en grupos

Grupo requerido (opcional). Introduzca el nombre distinguido completo de un grupo para los usuarios de Internet autorizados.

Además de una correcta autenticación, se requerirá la pertenencia a este grupo para acceder a la web.

Nota

Si el nombre del grupo contiene espacios, debe "preceder" estos espacios con una barra invertida.

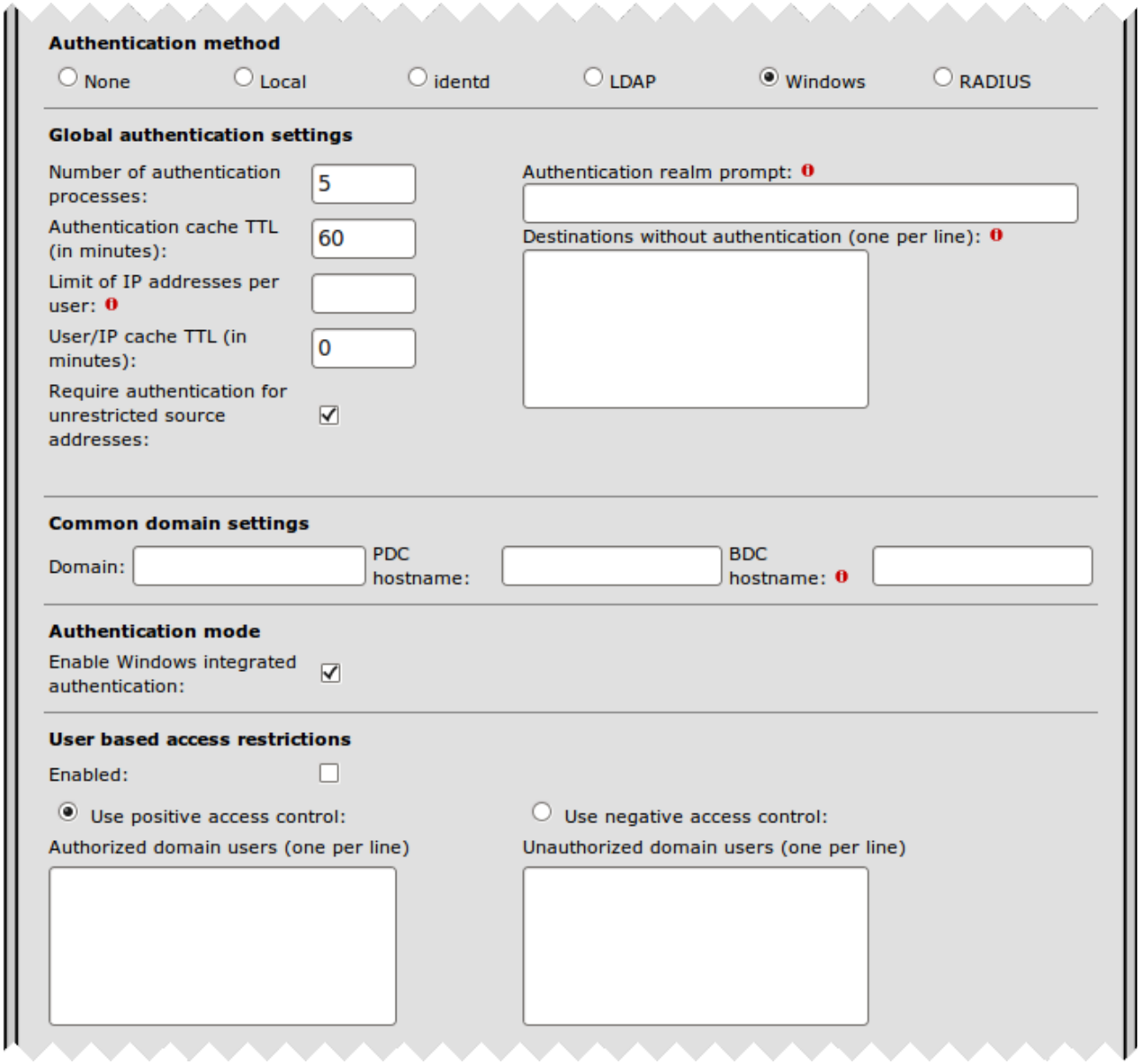
2.10.4. Autenticación Windows

Este método de autenticación es adecuado para entornos de red pequeños y medianos. Los usuarios tienen que autenticarse cuando acceden a sitios web. Las credenciales se verifican contra un servidor externo que actúa como Controlador de Dominio. Éste puede ser un:

- Servidor Windows NT 4.0 o Windows 2000/2003/2008 Server (incluso con Directorio Activo activado).

- Servidor Samba 2.x / 3.x (corriendo como Controlador de Dominio).

El Proxy Avanzado funciona con la autenticación integrada de Windows (transparente) o con autenticación estándar (explícita, con nombre de usuario y contraseña).

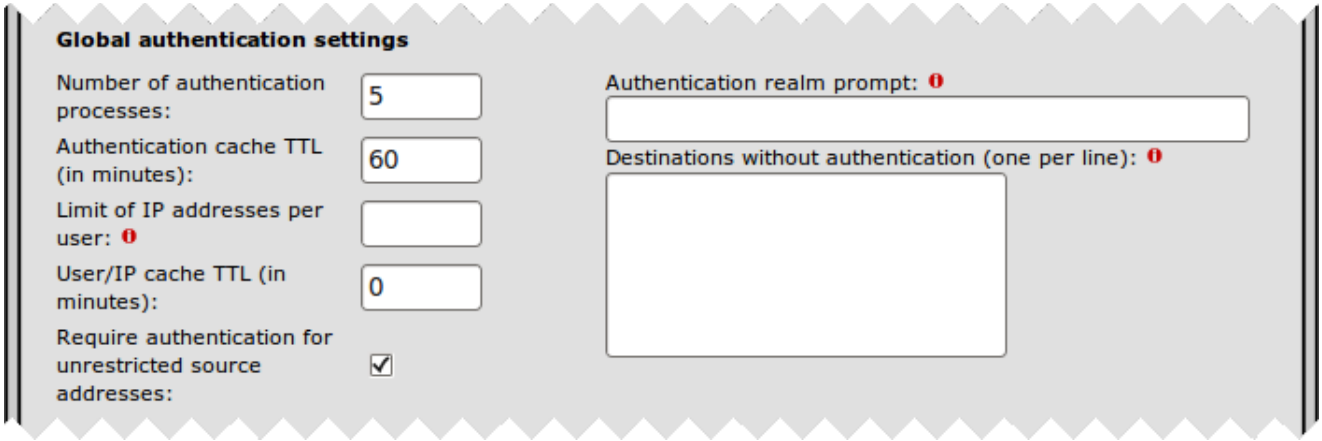


Puede mantener listas con nombres de usuario autorizados (lista blanca) o con nombres de usuario denegados (lista negra).

Nota

La autenticación basada en Grupo de Trabajo probablemente funcione, pero ni se recomienda ni está soportada.

2.10.4.1. Ajustes de autenticación globales



Número de procesos de autenticación. El número de procesos en segundo plano a la escucha de peticiones. El valor por defecto es 5 y debería ser incrementado si la autenticación toma demasiado tiempo o la autenticación integrada de Windows pasa a autenticación explícita.

TTL de la caché de autenticación. El tiempo en minutos durante el cual las credenciales se mantendrán en caché para cada sesión. Si este tiempo expira, el usuario tiene que volver a introducir las credenciales para esa sesión. Por defecto es de 60 minutos, el mínimo es de 1 minuto. El TTL se reinicia cada vez que el usuario envía una petición al servidor Proxy durante una sesión.

Nota

Si el usuario abre una nueva sesión, las credenciales siempre tienen que ser introducidas, incluso si el TTL no ha expirado para otra sesión.

Límite de direcciones IP por usuario (opcional). Número de direcciones IP de origen desde las que un usuario puede estar autenticado a la vez. La dirección IP se liberará tras el tiempo establecido en *TTL de la caché de Usuario/IP.*

Nota

Esto no tiene efecto si se está usando autenticación Local y el usuario es miembro del grupo *Extendido*.

TTL de la caché de Usuario/IP. Tiempo en minutos durante el cual se mantendrán en caché las relaciones entre cada usuario y la dirección IP empleada. El valor por defecto es 0 (desactivado).

Un valor mayor de 0 sólo tiene sentido cuando se emplea un límite de direcciones IP concurrentes por usuario.

Requerir autenticación para direcciones de origen no restringidas. Por defecto se requiere autenticación incluso para las direcciones IP no restringidas. Si no quiere requerir autenticación a esas direcciones, desmarque esta casilla.

Texto del diálogo de autenticación. Este texto se mostrará en el diálogo de autenticación. Por defecto es “Servidor Proxy Avanzado de IPCop”

Destinos sin autenticación. Esto le permite definir una lista de destinos que pueden ser accedidos sin autenticación.

Nota

Cualquier dominio listado aquí son dominios de destino DNS y no dominios de origen Windows NT.

Ejemplos:

Dominios completos y subdominios

```
*.ejemplo.net
*.google.com
```

Hosts únicos

```
www.ejemplo.net
www.google.com
```

Direcciones IP

```
81.169.145.75
74.125.39.103
```

URLs

```
www.ejemplo.net/download
www.google.com/images
```

Nota

Puede introducir todos estos tipos de destino en cualquier orden.

Ejemplo para Windows Update.

Para permitir acceder a Windows Update sin autenticación añada estos destinos a la lista:

```
*.download.microsoft.com
*.windowsupdate.com
windowsupdate.microsoft.com
```

2.10.4.2. Ajustes comunes de dominio

Dominio. Introduzca el nombre del dominio que quiere utilizar para la autenticación. Si está corriendo un Directorio Activo de Windows 2000 o Windows 2003, deberá introducir el nombre de dominio NetBIOS.

Nombre del CPD. Introduzca el nombre NetBIOS del Controlador Primario de Dominio aquí. Si está corriendo un Directorio Activo de Windows 2000 o Windows 2003, puede introducir el nombre de cualquier Controlador de Dominio.

Nota

En Windows 2000 y posteriores, el Controlador Primario de Dominio no está asignado a un servidor específico. El emulador de CPD de Directorio Activo es un rol lógico y puede estar asignado a cualquier servidor.

Importante

El nombre del CPD debe poder resolverse por IPCop. Esto se puede lograr añadiendo el nombre de host en Servicios > Editar Hosts (recomendado) o editando el archivo `/etc/hosts` directamente.

Nombre del CDR (opcional). Introduzca el nombre NetBIOS del Controlador de Dominio de Reserva aquí. Si está corriendo un Directorio Activo de Windows 2000 o Windows 2003, puede introducir el nombre de cualquier Controlador de Dominio. Si el CPD no responde a las peticiones de autenticación, el proceso de autenticación consultará al CDR en su lugar.

Importante

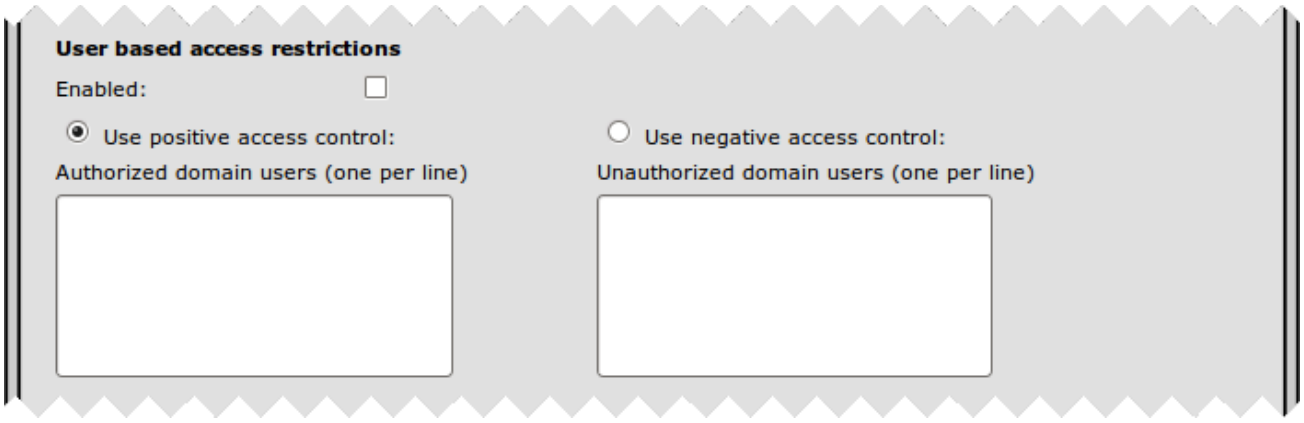
El nombre del CDR debe poder resolverse por IPCop. Esto se puede lograr añadiendo el nombre de host en Servicios > Editar Hosts (recomendado) o editando el archivo `/etc/hosts` directamente.

2.10.4.3. Modo de autenticación

Activar autenticación integrada de Windows. Si está activada, no se le preguntará al usuario por el nombre de usuario y contraseña. Se usarán las credenciales del usuario actualmente activo automáticamente para la autenticación. Esta opción está activada por defecto.

Si la autenticación integrada está desactivada, se le pedirá explícitamente al usuario un nombre de usuario y contraseña.

2.10.4.4. Restricciones basadas en usuario



Activado. Activa las listas de control de acceso para usuarios autorizados o denegados.

Utilizar control de acceso positivo / Usuarios de dominio autorizados. Los usuarios listados aquí tendrán acceso web. Para todos los demás usuarios, el acceso será denegado.

Utilizar control de acceso negativo / Usuarios de dominio denegados. Los usuarios listados aquí tendrán el acceso web bloqueado. Para todos los demás usuarios, el acceso estará permitido.

Nota

Si la autenticación integrada de Windows está activada, el nombre de usuario debe ser introducido con el nombre de dominio como prefijo, separado por una barra invertida.

Ejemplo de listas de control de acceso por usuario usando autenticación integrada:

```
dominio\administrador
dominio\bruno
dominio\juana
dominio\maria
dominio\pablo
dominio\esteban
```

Nota

Cuando se usa la autenticación integrada, el usuario tiene que estar logeado en el dominio, de lo contrario, se añadirá el nombre de la máquina al nombre de usuario, en vez de el nombre de dominio.

Ejemplo de listas de control de acceso por usuario usando autenticación explícita:

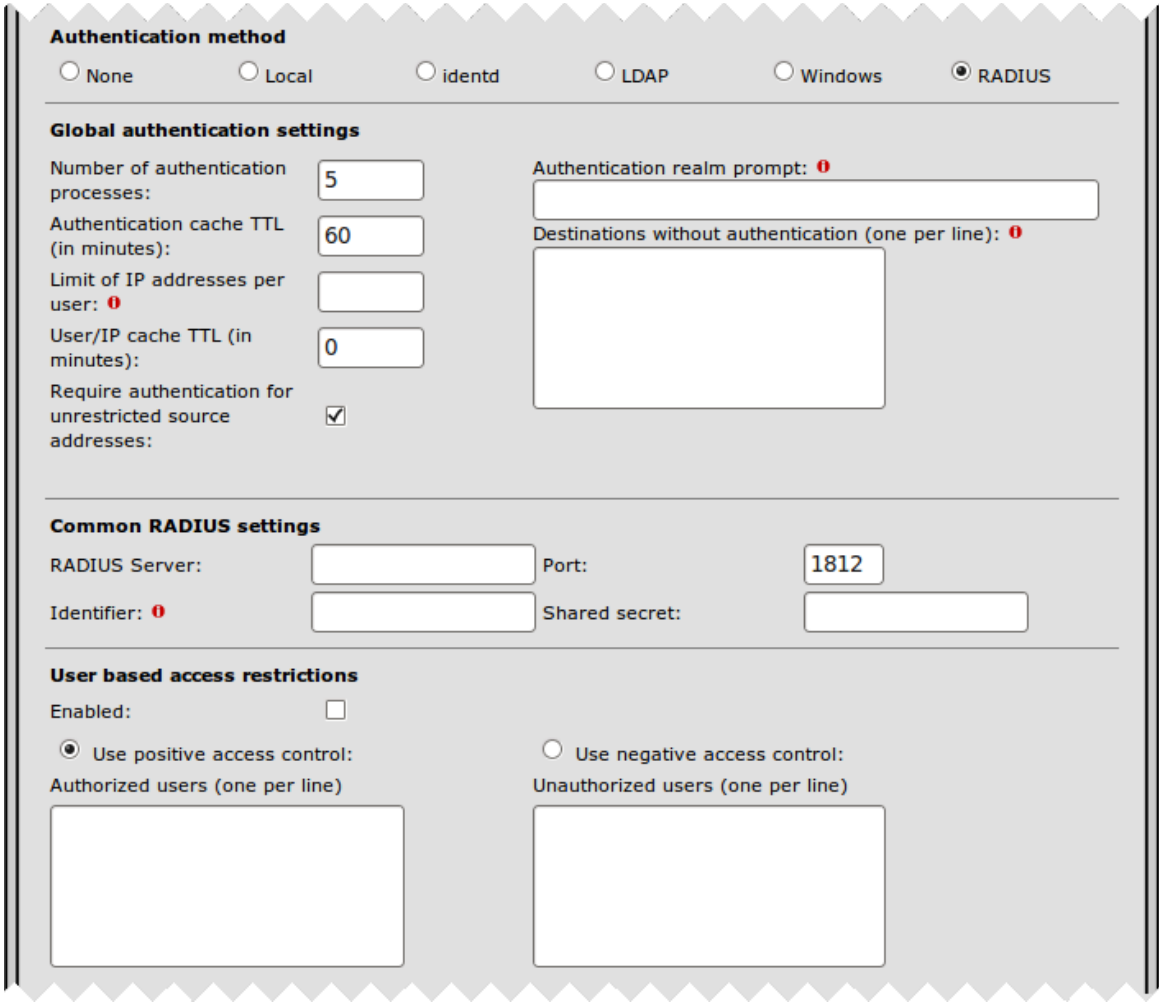
```
administrador
bruno
juana
maria
pablo
esteban
```

Nota

La autenticación explícita proporciona acceso al usario, incluso si el usuario no está logeado en el dominio, siempre que el nombre de usuario sea el mismo y que la contraseña de la máquina local y la contraseña de dominio no coincidan.

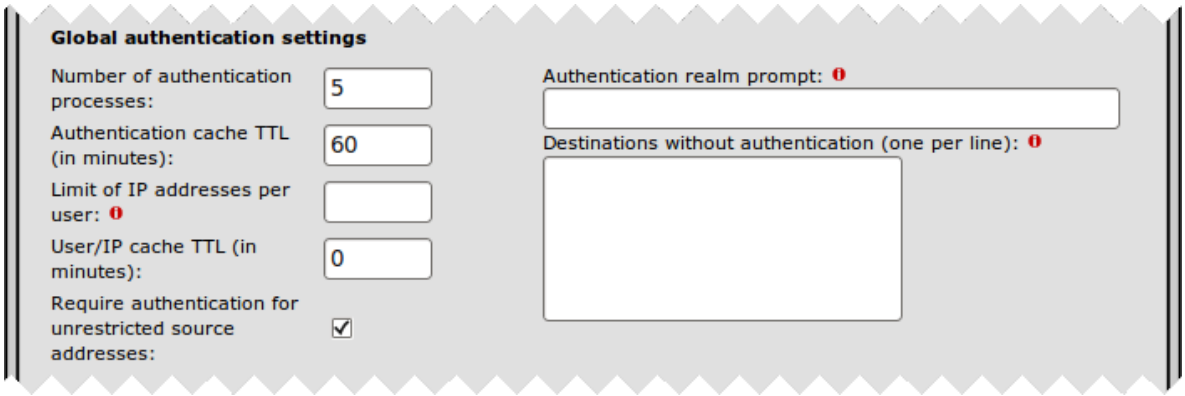
2.10.5. Autenticación RADIUS

Este método de autenticación es adecuado para entornos de red pequeños y medianos. Los usuarios tienen que autenticarse cuando acceden a sitios web. Las credenciales se verifican contra un servidor RADIUS externo.



Además de la autenticación, puede definir listas de control de acceso por usuario positivas (lista blanca) o denegadas (lista negra).

2.10.5.1. Ajustes de autenticación globales



Número de procesos de autenticación. El número de procesos en segundo plano a la escucha de peticiones. El valor por defecto es 5 y debería ser incrementado si la autenticación toma demasiado tiempo o la autenticación integrada de Windows pasa a autenticación explícita.

TTL de la caché de autenticación. El tiempo en minutos durante el cual las credenciales se mantendrán en caché para cada sesión. Si este tiempo expira, el usuario tiene que volver a introducir las credenciales para esa sesión. Por defecto es de 60 minutos, el mínimo es de 1 minuto. El TTL se reinicia cada vez que el usuario envía una petición al servidor Proxy durante una sesión.

Nota

Si el usuario abre una nueva sesión, las credenciales siempre tienen que ser introducidas, incluso si el TTL no ha expirado para otra sesión.

Límite de direcciones IP por usuario (opcional). Número de direcciones IP de origen desde las que un usuario puede estar autenticado a la vez. La dirección IP se liberará tras el tiempo establecido en *TTL de la caché de Usuario/IP.*

Nota

Esto no tiene efecto si se está usando autenticación Local y el usuario es miembro del grupo *Extendido*.

TTL de la caché de Usuario/IP. Tiempo en minutos durante el cual se mantendrán en caché las relaciones entre cada usuario y la dirección IP empleada. El valor por defecto es 0 (desactivado).

Un valor mayor de 0 sólo tiene sentido cuando se emplea un límite de direcciones IP concurrentes por usuario.

Requerir autenticación para direcciones de origen no restringidas. Por defecto se requiere autenticación incluso para las direcciones IP no restringidas. Si no quiere requerir autenticación a esas direcciones, desmarque esta casilla.

Texto del diálogo de autenticación. Este texto se mostrará en el diálogo de autenticación. Por defecto es “Servidor Proxy Avanzado de IPCop”

Destinos sin autenticación. Esto le permite definir una lista de destinos que pueden ser accedidos sin autenticación.

Nota

Cualquier dominio listado aquí son dominios de destino DNS y no dominios de origen Windows NT.

Ejemplos:

Dominios completos y subdominios

```
*.ejemplo.net
*.google.com
```

Hosts únicos

```
www.ejemplo.net
www.google.com
```

Direcciones IP

```
81.169.145.75
74.125.39.103
```

URLs

```
www.ejemplo.net/download
www.google.com/images
```

Nota

Puede introducir todos estos tipos de destino en cualquier orden.

Ejemplo para Windows Update.

Para permitir acceder a Windows Update sin autenticación añada estos destinos a la lista:

```
*.download.microsoft.com
*.windowsupdate.com
windowsupdate.microsoft.com
```

2.10.5.2. Ajustes comunes de RADIUS

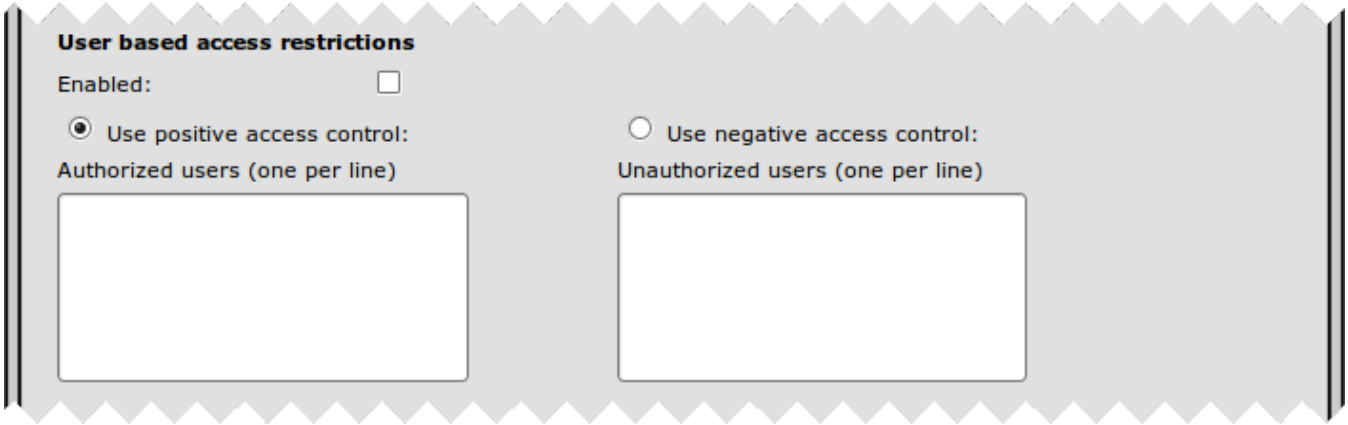
Servidor RADIUS. Introduzca la dirección IP del servidor RADIUS que quiere usar para la autenticación.

Puerto. Introduzca el puerto que será empleado para comunicarse con el servidor RADIUS. El puerto por defecto es el 1812, algunos servidores RADIUS pueden emplear el puerto 1645 en su lugar.

Identificador (opcional). Este es un campo opcional y se puede usar para identificar su IPCop ante el servidor RADIUS. Si se deja en blanco, se usará la dirección IP de su IPCop para la identificación.

Secreto compartido. Este es el secreto compartido para la autenticación de su IPCop contra el servidor RADIUS. Esta debe ser la misma contraseña que ha introducido en el servidor RADIUS.

2.10.5.3. Restricciones basadas en usuario



Activado. Activa las listas de control de acceso para usuarios autorizados o denegados.

Utilizar control de acceso positivo / Usuarios autorizados. Los usuarios listados aquí tendrán acceso web. Para todos los demás usuarios, el acceso será denegado.

Utilizar control de acceso negativo / Usuarios denegados. Los usuarios listados aquí tendrán el acceso web bloqueado. Para todos los demás usuarios, el acceso estará permitido.

2.10.6. Extensiones de aula

Las Extensiones de Aula (EA) del servidor proxy le ofrecen la posibilidad de delegar tareas administrativas a usuarios no administrativos mediante una página de Gestión de Acceso Web separada.

Las EA ofrecen estas prestaciones:

Gestión de acceso completamente basada en web

- Grupos de clientes predefinidos que se pueden activar o desactivar usando un navegador estándar.
- Todas las opciones administrativas de las EA son accesibles y configurables en la GUI web de IPCop.

Diferentes niveles de seguridad

- Los derechos de Gestión de Acceso Web se pueden controlar mediante contraseña y/o por dirección de red.
- No se necesitan privilegios administrativos en la GUI de IPCop para la Gestión de Acceso Web.
- El supervisor no puede saltarse ninguna restricción del servidor proxy impuesta por el Administrador de IPCop.

Configuración flexible

- El Administrador de IPCop puede definir grupos de clientes mediante direcciones MAC, direcciones IP únicas, rangos de IPs, subredes o incluso todas ellas.

Las EA crean un nuevo rol, entre el Administrador y los Usuarios: el Supervisor.

El supervisor puede activar o desactivar el acceso web para grupos predefinidos (p.e. ordenadores concretos en un aula) sin la necesidad de tener derechos de acceso o conocimientos administrativos de la GUI de IPCop.

La interfaz de Gestión de Acceso Web puede ser iniciada desde cualquier ordenador cliente. Abra un navegador e introduzca la URL https://192.168.1.1:8443/cgi-bin/webaccess.cgi (reemplazando el 192.168.1.1 con la dirección de su IPCop).

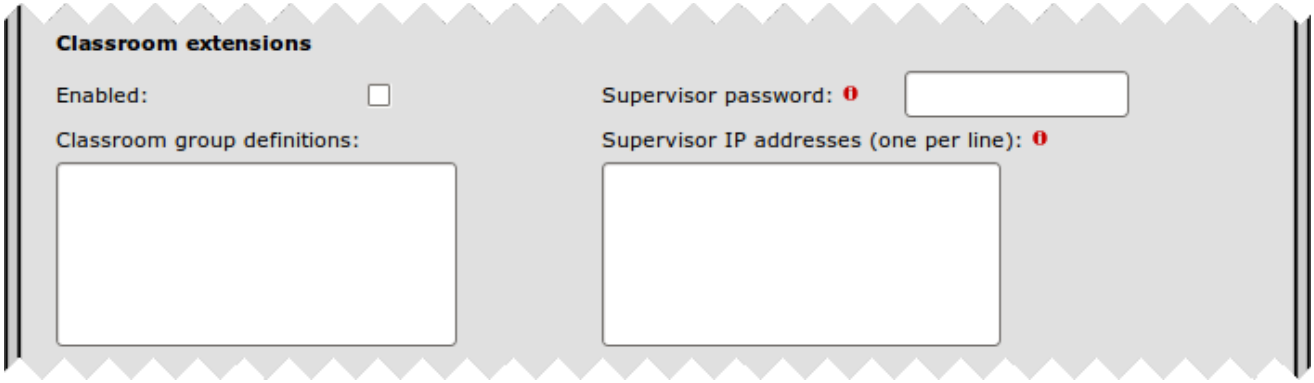
Si la Interfaz de Gestión de Acceso Web no ha sido activada por el Administrador, verá el siguiente texto: “La interfaz de gestión ha sido deshabilitada por el Administrador”.

Si la Interfaz de Gestión de Acceso Web ha sido activada, pero el Administrador no ha definido ningún grupo, verá este texto: “No hay grupos de acceso disponibles”.

2.10.6.1. Configuración de extensiones de aula

Las extensiones de aula se activan, desactivan y configuran en la página servidor proxy.

Tras realizar cualquier cambio, recuerde pulsar el botón Guardar para aplicarlo.



Activado. Marque esta casilla para activar el Supervisor de la Interfaz de Gestión de Acceso Web.

Contraseña del Supervisor (opcional). Cuando se pone esta contraseña, todos los Supervisores deben introducirla para gestionar el acceso web. Esto es opcional, pero por razones de seguridad, defina una contraseña de Supervisor o direcciones IP de Supervisor.

Direcciones IP de Supervisor (una por línea) (opcional). Este campo le permite definir las direcciones IP que podrán gestionar el acceso web. Esto es un elemento de configuración opcional que puede emplearse para incrementar la seguridad o para simplificar el mantenimiento, si no quiere configurar una contraseña de Supervisor.

Por ejemplo, añada estas direcciones IP si quiere permitirles acceso de supervisor:

```
192.168.1.20
192.168.1.30
```

El mayor nivel de seguridad se alcanza cuando se definen tanto una contraseña de Supervisor como restricciones por IP, como se describe en la sección Niveles de seguridad de EA.

Definiciones de grupos de aula. Sus definiciones de grupos de aula se introducen en este campo. Una definición de grupo de aula tiene este formato:

```
[nombredegrupo]
direccion MAC cliente o dirección IP cliente o rango IP o subred IP
direccion MAC cliente o dirección IP cliente o rango IP o subred IP
direccion MAC cliente o dirección IP cliente o rango IP o subred IP
```

Así que, por ejemplo, puede tener un par de definiciones de grupo como estas:

```
[Grupo ejemplo 1]
192.168.1.11
192.168.1.12
192.168.1.13
[Grupo ejemplo 2]
192.168.1.21-192.168.1.25
```

Cada grupo tiene un 'nombredegrupo', que debe ser único. El nombre de grupo es la parte de la definición de grupo entre corchetes. El nombre aparecerá en la interfaz de gestión de acceso web.

Cada grupo puede tener un número ilimitado de definiciones de clientes. Puede usar definiciones de clientes mezcladas dentro de un grupo, pero cada definición tiene que estar en una sola línea. Aquí hay algunos ejemplos:

Host único - Dirección MAC

```
01:23:45:67:89:0A
```

Host único - Dirección IP

```
192.168.1.11
```

Rango de hosts

`192.168.1.21-192.168.1.25`

Subred (notación de máscara de red)

`192.168.1.32/255.255.255.240`

Subred (notación CIDR)

`192.168.1.32/28`

2.10.6.2. Niveles de seguridad de EA

Nivel 1: Sin contraseña, sin restricciones por IP - sin seguridad. Todos los clientes podrán gestionar el acceso web sin ninguna restricción. Esto no se recomienda para entornos de producción.

Nota

¡Utilice esto sólo con propósitos de diagnóstico o prueba!

Nivel 2: Contraseña definida, sin restricciones por IP - seguridad baja. Todos los clientes podrán gestionar el acceso web, pero se requerirá una contraseña para guardar los cambios. Este nivel de seguridad se recomienda en un entorno sin ordenadores dedicados al Supervisor.

Nivel 3: Sin contraseña, restricciones por IP aplicadas - seguridad baja. Todos los clientes listados aquí podrán cambiar los ajustes de acceso web. Los clientes se identificarán mediante su dirección IP, no se requiere contraseña para guardar los cambios.

Nota

Si la dirección IP del cliente no está listada aquí, la interfaz de gestión de acceso web aparecerá en modo “sólo-visualizar”.

Nivel 4: Contraseña definida, restricciones por IP aplicadas - seguridad alta. Este es el nivel más alto de seguridad para la interfaz de gestión de acceso web. Sólo los clientes listados pueden cambiar los ajustes, se requerirá una contraseña para guardar los cambios.

Nota

Si la dirección IP del cliente no está listada aquí, la interfaz de gestión de acceso web aparecerá en modo “sólo-visualizar”.

Apéndice A. GNU Free Documentation License

Version 1.2, November 2002

Tabla de contenidos

A.1. 0. Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

A.2. 1. Applicability and Definitions

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “Modified Version” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

A.3. 2. Verbatim Copying

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

A.4. 3. Copying In Quantity

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

A.5. 4. Modifications

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section entitled “History”, Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled “History” in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the “History” section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. In any section Entitled “Acknowledgements” or “Dedications”, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled “Endorsements”. Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made `by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

A.6. 5. Combining Documents

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements.”

A.7. 6. Collections of Documents

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

A.8. 7. Aggregation With Independent Works

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

A.9. 8. Translation

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warrany Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

A.10. 9. Termination

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

A.11. 10. Future Revisions of This License

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See the GNU Free Documentation License web site.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.