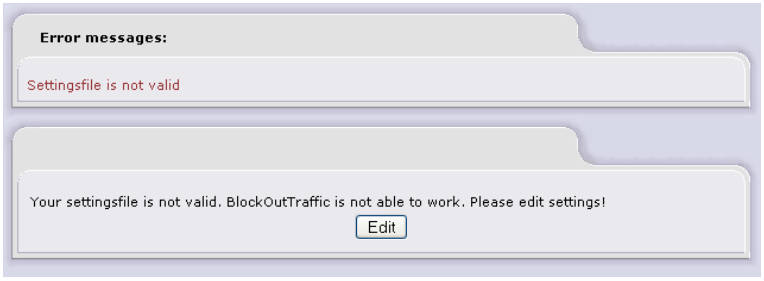
Iniciando a configuração do BOT

Traduzido por: Antonio Edivaldo de O. Gaspar, edivaldo.gaspar(at)gmail(dot)com
Texto original: http://www.blockouttraffic.de/gettingstarted.php
Revisado em: 25/07/06 – 09:00

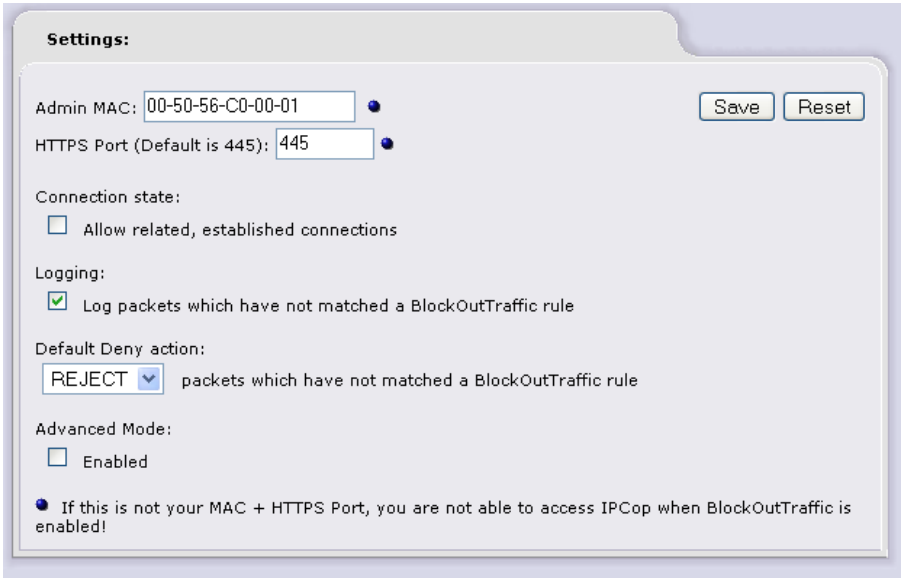
Passos iniciais

Após instalar o BlockOutTraffic, o seu menu de configuração estará disponível na página de administração do IPCop. Antes de ser ativado, é preciso configurar o BOT para permitir acesso ao *host* que será usado na sua administração (preferencialmente neste passo, utilize um computador localizado na rede interna - GREEN).

Na página do IPCop vá em Firewall > BlockOutTraffic. A página ilustrada abaixo será exibida solicitando a edição das configurações iniciais do BOT:



Clique no botão [EDIT] e preencha os campos da seção "BOT settings", como descrito a seguir:



Admin MAC: este campo deve ser preenchido com o “MAC address” do computador que irá administrar o IPCop.

HTTPS Port: identifique a porta de conexão da página do IPCop (445/TCP).

Connection state: habilitando esta opção, o BOT permitirá o tráfego pertencente a uma conexão existente (conexão relacionada ou estabelecida) ou um pacote originado em resposta a outro. Caso você esteja usando o Port-Forward (p. ex. a um Web-server interno) marque esta opção.

Logging: habilite este item para criar um registro ou Log para o tráfego que não combinar com suas regras.

Default Deny action: Nesta opção, você pode selecionar qual será a ação Deny a ser tomada pelo BOT com o tráfego que não combinar com uma de suas regras: DROP ou REJECT .

```
Relembrando:
Drop: não permite a passagem do pacote, descartando-o. Não avisa a origem sobre o ocorrido.
Reject: igual ao DROP, mas avisa a origem sobre o ocorrido (envia um pacote ICMP unreachable).
```

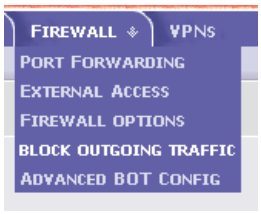
Advanced Mode: Marcando a opção “Advanced Mode”, na página de criação de regras, mais opções estarão disponíveis para *customizar* as necessidades do cliente às regras de BOT. Mas é importante adverti-lo que você pode abrir seu Firewall habilitando o modo avançado! Você só deve selecionar esta opção se possuir bastante conhecimento sobre o funcionamento do Firewall.

Clique em [SAVE] para armazenar as configurações e, a partir deste ponto, você já pode começar a definir as regras de BOT e outras características para trabalhar o tráfego no seu Firewall.

Ao finalizar o cadastro da seção “Settings”, o BlockOutTraffic cria uma regra de acesso administrativo (*default admin access rule*) para o MAC, como endereço de origem, e “IPCop/HTTPS Port”como destino. Isso garante que você não irá perder o acesso à página de administração do IPCop quando o BOT for ativado. Esta é razão de você preencher os campos Admin MAC e HTTPS Port. A observação no final da figura acima destaca a importância deste cadastro: se os campos “MAC + HTTPs Port” não forem preenchidos corretamente, você perderá o acesso ao IPCop quando o BlockOutTraffic for habilitado !

Advanced BOT Config

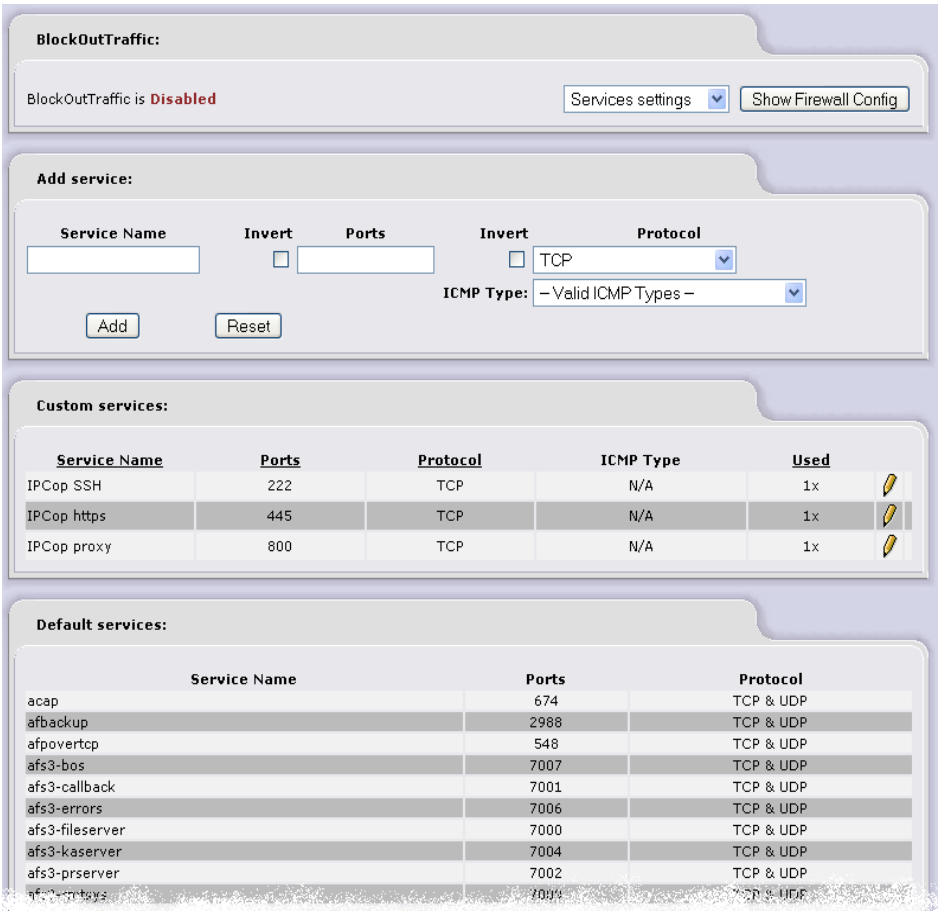
Uma vez configurado o acesso administrativo ao IPCop, podemos iniciar o cadastro de serviços e endereços. Identificamos serviços e endereços como objetos que guardam informações globais sobre “números de portas/protocolos” e “endereços de hosts”, respectivamente. Tais objetos podem ser manipulados em regras ou ainda serem agrupados, representando assim uma categoria específica. Para iniciar o gerenciamento de serviços e endereços, vá no menu "Firewall > Advanced BOT Config".



Service Settings

Em primeiro lugar, aprenderemos a definir alguns serviços não disponíveis na configuração do BOT. O cadastro desses serviços será de grande utilidade quando você for adicionar as regras do seu Firewall.

Na seção "Default Services" que exibimos na figura a seguir, estão listados os serviços cadastrados por padrão no BOT.



Como observamos na figura anterior, há três serviços em “Custom Services”. Estes serviços estão relacionados às portas SSH, HTTPS e Proxy Web, de acesso ao IPCop. Para liberar o acesso ao Firewall a outros computadores, além daquele especificado na Página "BOT settings", precisamos cadastrar as portas SSH e HTTPS. Uma vez feito o cadastro, as mesmas estarão disponíveis na página de cadastro de regras.

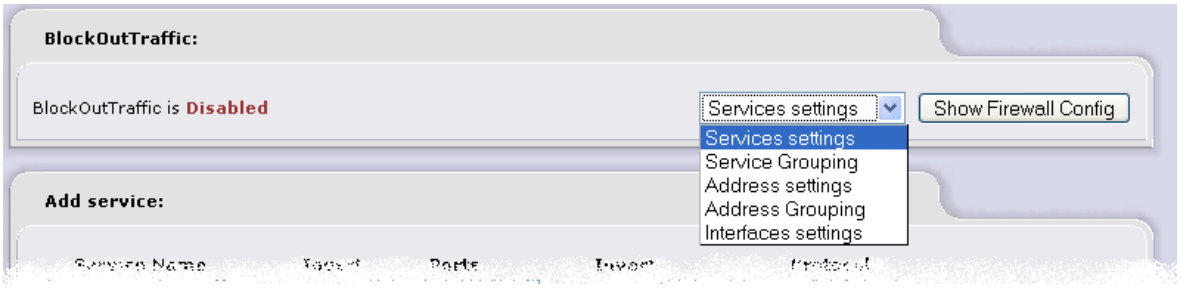
Os serviços acima citados foram adicionados através da seção "Add Service", através dos campos “Service Name”, “Ports” e “Protocol”. Os detalhes sobre cada serviço são descritos a seguir:

- IPCop ssh: porta ssh do IPCop (222/TCP), necessária para administrar seu IPCop via conexão ssh.
- IPCop https (445/TCP): acesso SSL à página administrativa do IPCop.
- IPCop Proxy: faça o cadastro da porta do Proxy Web do IPCop (800/TCP). Isto é feito para permitir que o Proxy do IPCop seja utilizado pela rede interna (GREEN). A porta do Proxy deve ser cadastrada para estar disponível no momento que você for criar uma regra para permitir que os usuários da sua rede naveguem na Internet via Webproxy. O cadastro deste serviço é importante, caso seja utilizado o recurso de Proxy Transparente do IPCop.

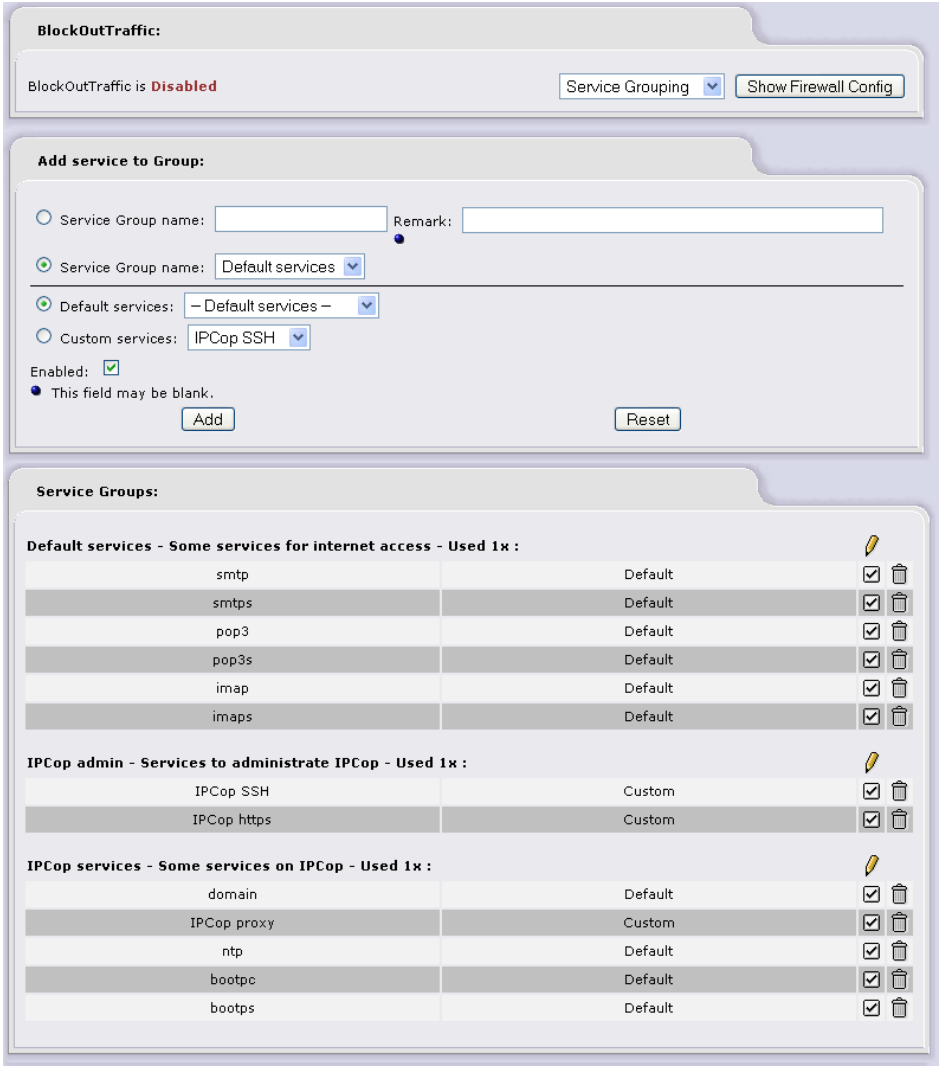
Além do cadastro você também pode agrupar serviços em um único objeto, ou criar outros objetos como endereços (IP ou MAC) e interfaces. Estes recursos são descritos a seguir:

- Criar grupos de serviços (Service Grouping): agrupar os serviços cadastrados.
- Cadastro de hosts (Address Settings) através do endereço (IP ou MAC)
- Criar grupos de Endereços (Address Grouping): agrupar os objetos de endereço.
- adicionar uma nova interface: cadastrar uma nova interface (p. ex VPN).

Estas opções podem acessadas no menu dropdown visualizado na figura a seguir:



Para agrupar serviços, selecione opção “Service Grouping”, a página a seguir será exibida:



Na figura anterior foram definidos os seguintes grupos:

- Default services: contêm serviços que os *hosts* da sua rede podem querer acessar na Internet (neste exemplo relacionados a correio eletrônico).
- IPCop admin (Administração do IPCop): contêm serviços (ou portas) relacionados a administração do IPCop. Este grupo pode ser usado convenientemente para permitir acesso à página de administração do IPCop a outros *hosts* além daquele definido no campo "Admin MAC" da seção "BOT settings".
- IPCop services: contêm serviços do tipo DNS, Proxy, NTP e DHCP. Este grupo pode ser usado para criar uma regra cujo objetivo seria permitir aos computadores da rede o acesso aos serviços do IPCop.

Depois de definir serviços, e grupos de serviços, nós já podemos cadastrar nossa

primeira regra no BOT. Em primeiro lugar, qual será a política de acesso para a nossa rede ? Que serviços queremos permitir aos *hosts* da rede interna (GREEN) ?

Supondo que desejamos que nossa rede acesse serviços do IPCop e da Internet, podemos usar a seguinte política de acesso:

- Enviar e receber emails;
- Surfar na Web via o Proxy do IPCop;
- Usar os serviços DNS, DHCP e NTP no IPCop;
- E mais tarde, para finalizar nosso trabalho, queremos permitir que dois *hosts* de nossa equipe de suporte acessem o IPCop via Página Web de Administração(445) e conexão SSH(222).

Obs: Lembre-se, a política padrão para o BOT é DROP (p.ex: da rede GREEN para a RED), para tanto, você deverá criar as regras que permitirão o tráfego citado acima.

Nós já definimos alguns serviços e grupos de serviços. Também definimos uma política básica de acesso, tanto de nossa rede à Internet quanto ao próprio Firewall. Assim, podemos cadastrar nossa primeira regra de BOT: disponibilizar os serviços do IPCop aos *hosts* de nossa rede. Volte a seção BlockOutTraffic (Firewall -> BlockOutTraffic) e clique na opção “New Rule” (Adicionar uma nova regra).

A página “New Rule” está dividida em quatro seções:

1. **Source (origem)**: identifica a origem do pacote com as opções.
   - Default Interface
   - “Adress Format” (IP ou MAC) e “Source Address” (Endereço de origem - IP/MAC)
   - Default Network: Rede de origem, padrão rede GREEN.
   - Custom Address: Endereços (hosts) cadastrados pelo usuário.
   - Address Group: Grupos de endereços (hosts) criados pelo usuário.
   - Invert (exclusão): altera o sentido da regra em relação ao endereço digitado, ou seja, serve para excluir o argumento da regra. No caso do endereço, refere-se a qualquer endereço de entrada, exceto o endereço ou grupo identificado.

2. **Destination(destino)**: identifica o destino do pacote com as opções
   - IPCop Access: o destino do é o Firewall IPCop
   - Other Network/Outside: outra rede, cujo padrão é Any(qualquer destino), Custom address (um host específico), Address Group (um grupo específico de hosts), Destination IP or Network(o campo pode ser preenchido com um endereço de um host ou rede).
   - Invert (exclusão): idêntico a opção Source. No caso do destino, refere-se a qualquer endereço de destino, exceto o endereço, rede ou grupo identificado.
   - Use Service: pode conter a opção “Service Groups” (quando o usuário cadastra grupos de serviços), “Custom Services” (para serviços cadastrados) e “Default Services” (para serviços cadastrados por padrão no IPCop).

3. **Additional(opções adicionais)**:
   - Rule enable(habilitar a regra): você pode apenas cadastrar a regra, sem no entanto, habilitá-la. Se marcar esta opção, a regra ficará ativa automaticamente após cadastro.
   - Log rule(Log da regra): marque esta opção se desejar registrar em Log o tráfego da regra.
   - Rule Action: Ação a ser aplicada à regra (ACCEPT ou DROP)
   - Remark: Comentário sobre a regra.

4. **Timeframe**: habilitando a opção “Add Timeframe” você pode escolher o intervalo de dias do mês, o dia a semana, ou intervalo de hora em que a regra estará ativa.

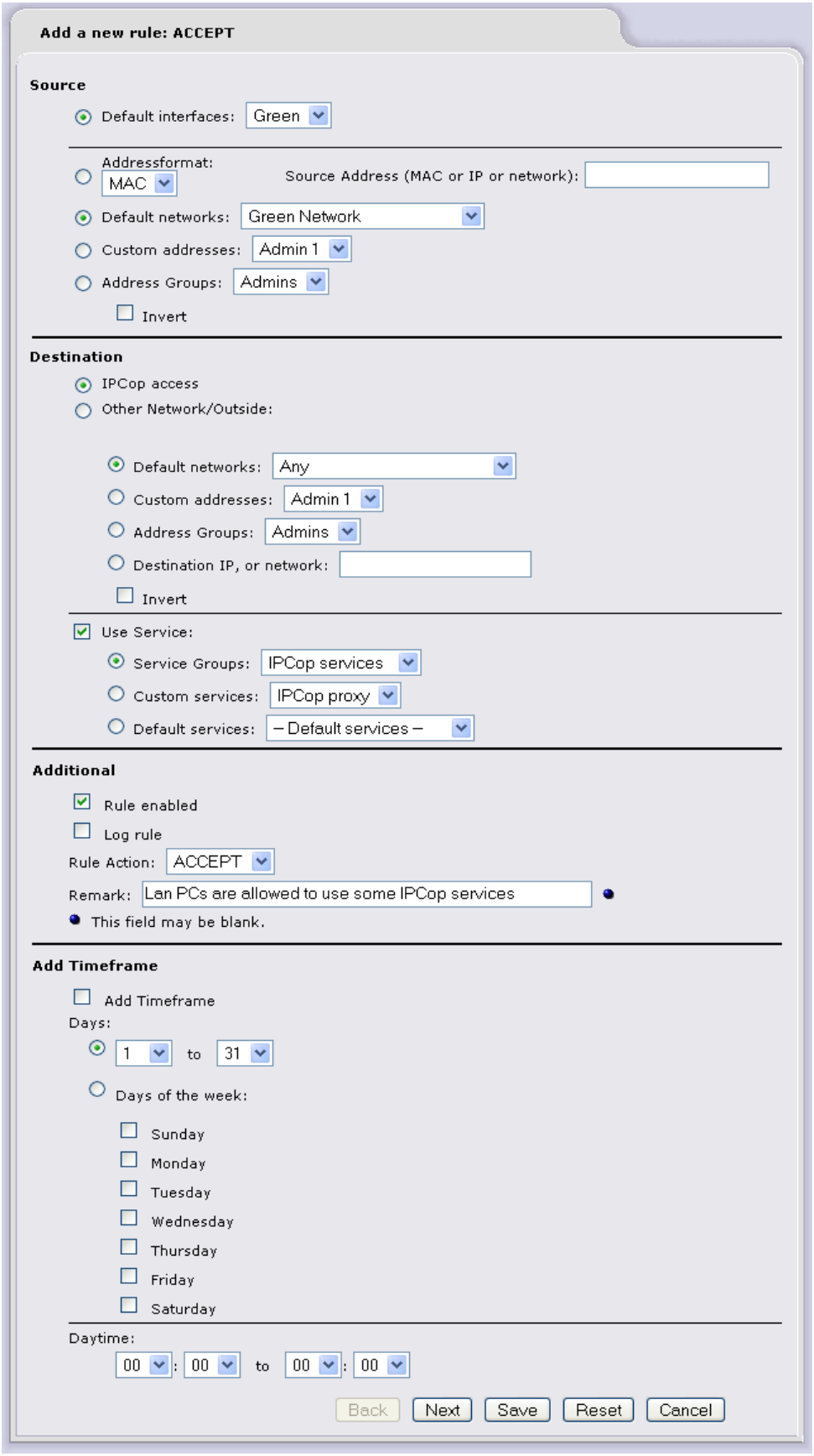
Obs: os campos seguidos por uma bola azul (●) são opcionais.

Assim, para permitir que a rede GREEN use os serviços do IPCop selecione:

Origem (source):
- Default interface: Green
- Default networks: Green Network

Destino (destination):
- IPCop access
- Marque a opção "use Service", e em "Service Group", escolha a opção "IPCop services" (o grupo que foi definido anteriormente para os serviços relacionados ao IPCop).

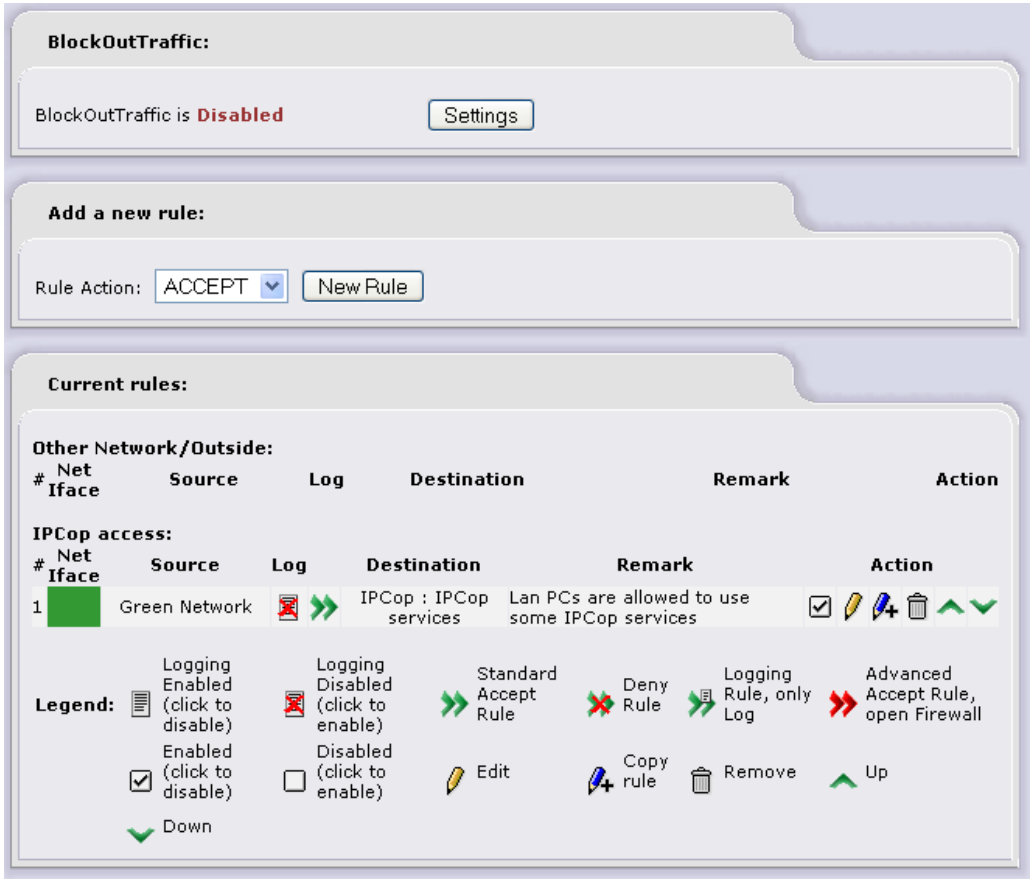
No campo “Remark”, digite um comentário sobre a regra.



A partir deste ponto, existem duas maneiras finalizar o processo de criação da regra: clicar em [Next] ou [Save]. A opção SAVE grava e adiciona a regra no final da lista do BlockOutTraffic. A opção NEXT exibirá uma prévia das opções da regra (origem, destino, serviço, ação, etc), possibilitando ainda selecionar em qual posição na lista a regra será inserida, veja a seguir:

Caso precise alterar alguma opção antes de salvar a regra, clique em [Back] para mudar uma opção. Uma vez terminado o cadastro, clique em [Save] para salvar a regra em uma posição específica. A princípio, a posição não é o que interessa, mas posteriormente, quando existirem muitas regras, você pode querer inserir uma regra em um ponto específico da lista.

Na seção "Current rules", você verá um resumo do que foi cadastrado, como exibido a seguir:



Como podemos observar na regra 1 da página acima, a política define que os serviços do IPCop estarão disponíveis para os *hosts* de sua LAN (rede GREEN).

Nossa tarefa agora é criar uma regra para permitir o acesso a serviços da Internet. Clique no Botão [New Rule] e selecione as seguintes opções:

Origem:

- Default interface: Green (Interface da Rede Interna)
- Default networks: Green Network (origem Rede Interna)

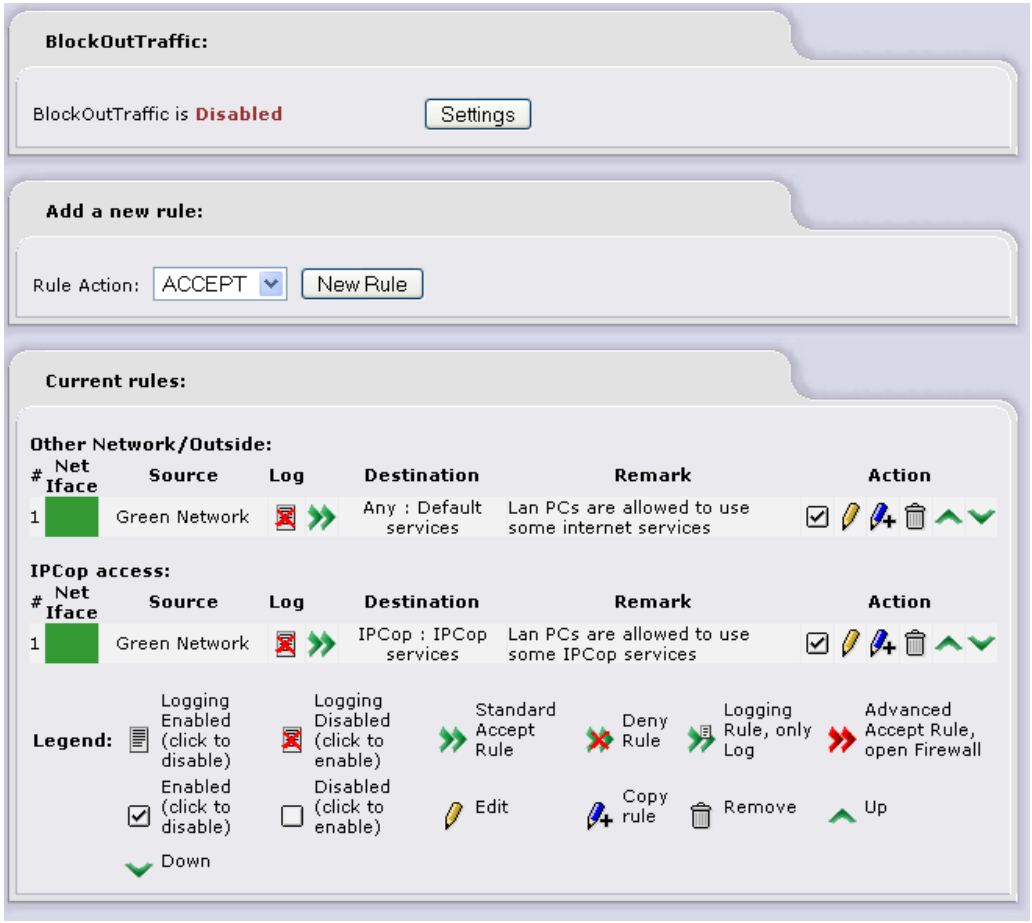
Destino:

- Other Network/Outside: Outra Rede/Exterior
- Default networks: Any (qualquer destino)
- Marque “Enable Services”: habilitar a regra por serviço, ou seja, qualquer destino (Any) para uma porta (ou portas/protocolos) específica.
- Selecione em Service Groups: Default services (o segundo grupo de serviços definido em “Service Grouping” do menu Advanced BOT Config)

Habilite a regra em “Rule Enable”. Clique em [Save] ou [Next]+[Save] e assim você gravará sua segunda regra no BlockOutTraffic.

Desta forma, os computadores da rede interna terão permissão para acessar serviços na Internet como Correio Eletrônico (você pode adicionar mais serviços ao grupo Default services) e usar o DNS, DHCP, NTP e Webproxy no IPCop.

Sua lista 'Current rules' exibirá as duas regras como a seguir:



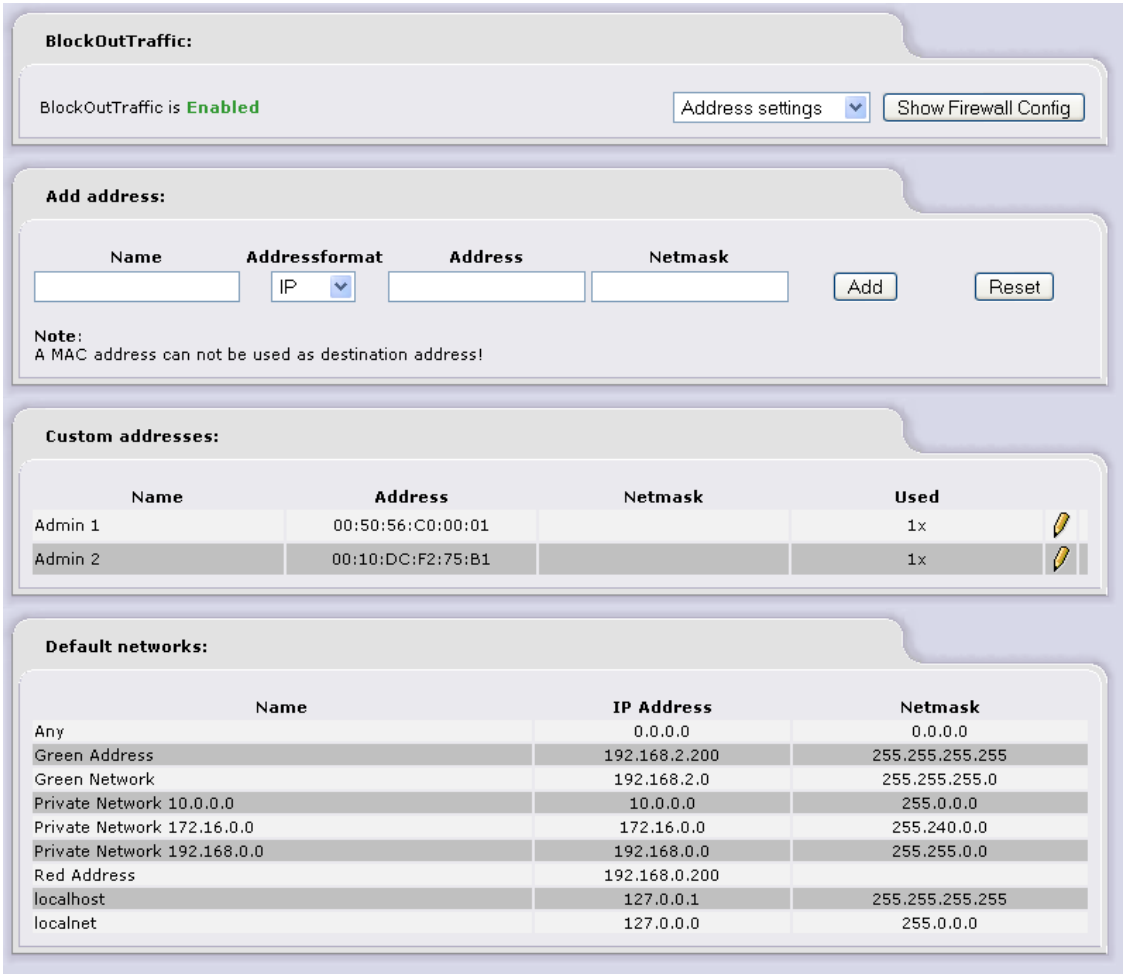
Você pode agora clicar no botão “Settings” depois marque a opção “BlockOutTraffic enabled” para habilitar o BOT. Todo tráfego que não é permitido por suas regras atuais é então bloqueado.

Se você deseja permitir a algum outro *host* o acesso para administrar o Firewall IPCop via Webgui ou SSH, veja próximo capítulo "Configurações Avançadas".

Configurações Avançadas

As primeiras regras de BOT foram definidas e agora podemos dar um passo adiante em nossa configuração. Assim, definiremos uma regra de BOT que permita as outros *hosts* da rede interna o acesso à página do IPCop.

Inicialmente, precisamos cadastrar os endereços MAC das maquinas que farão parte desta regra. Vá na página Advanced BOT Config e escolha “Address Settings”:

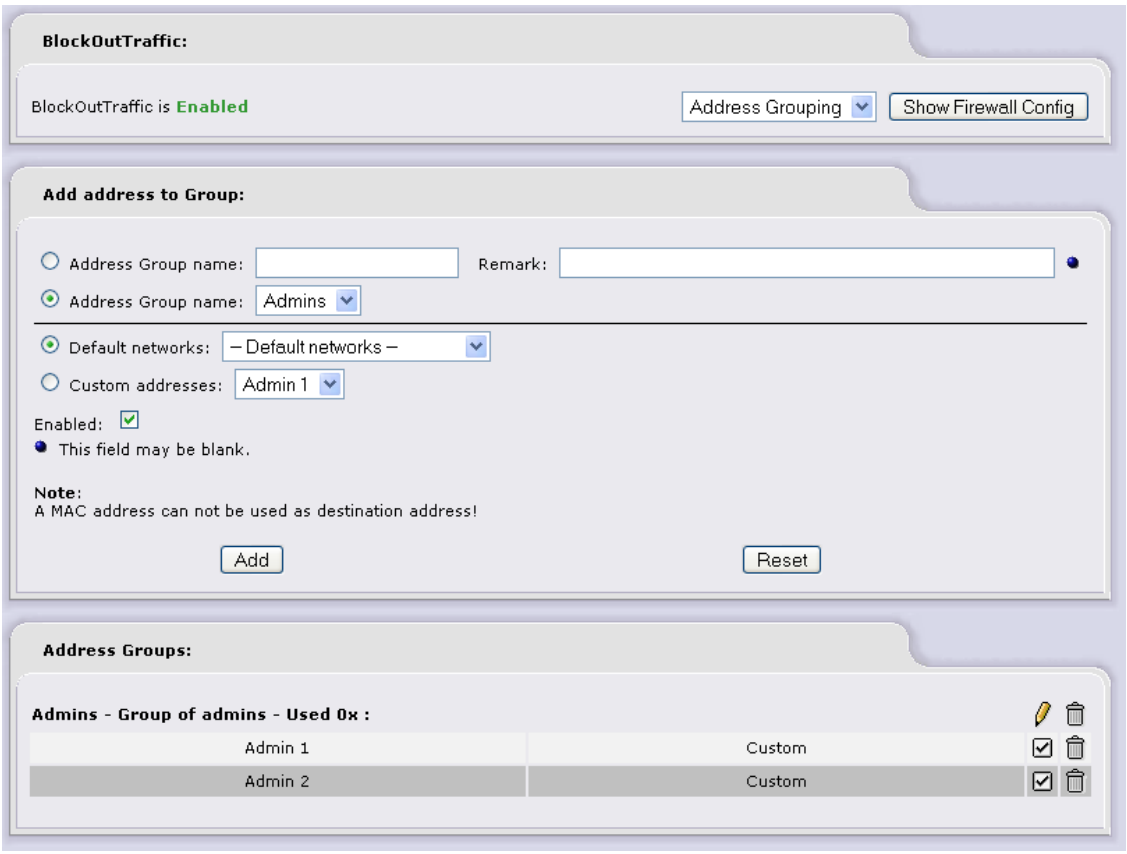


Acima, observamos que foram cadastros dois *hosts* que farão parte da administração(Admin 1 e Admin 2). Como podemos observar, os mesmos serão identificados pelo MAC Address, como uma forma de evitar a falsificação do acesso através de IP *spoffing*. Semelhante ao cadastro de serviços, endereços ou hosts também estarão presentes no momento de criação da regra. Agrupa-los em um único objeto que represente os hosts, é uma ótima opção para poupar trabalho no cadastro da regra.

Para criar um grupo de endereços (usando IPs ou MAC address), vá em “Advanced Config BOT” e escolha a opção de menu drop-down “Address Grouping” (visto na figura a seguir).

Clique na opção "Address Group name" e preencha o campo ao lado com o nome do grupo que deseja criar. Para este exemplo criamos o grupo denominado "Admins". Observe que os endereços MAC cadastrados na seção anterior são exibidos no menu ao lado da opção "Custom addresses"; clique nesta opção, escolha o objeto Admin1 e, em seguida, clique em "Add". Repita esta operação para o objeto Admin2.

Se você procedeu conforme combinamos, o BOT exibirá uma tela semelhante a figura a seguir:



Agora já podemos criar a regra para o grupo Admins. Volte à página de BlockOutTraffic e clique [New Rule].

Entre com as opções necessárias para a regra.

Origem:

- Default interface: Green
- Address Group: Admins

Destino:

- IPCop access: o destino será o próprio Firewall
- Clique em “Enable Services”.
- Selecione “Service Group”: IPCop admin (o terceiro grupo definido em Advanced BOT config)

Isso é tudo ! Sua lista de regras agora deve estar semelhante a figura a seguir: