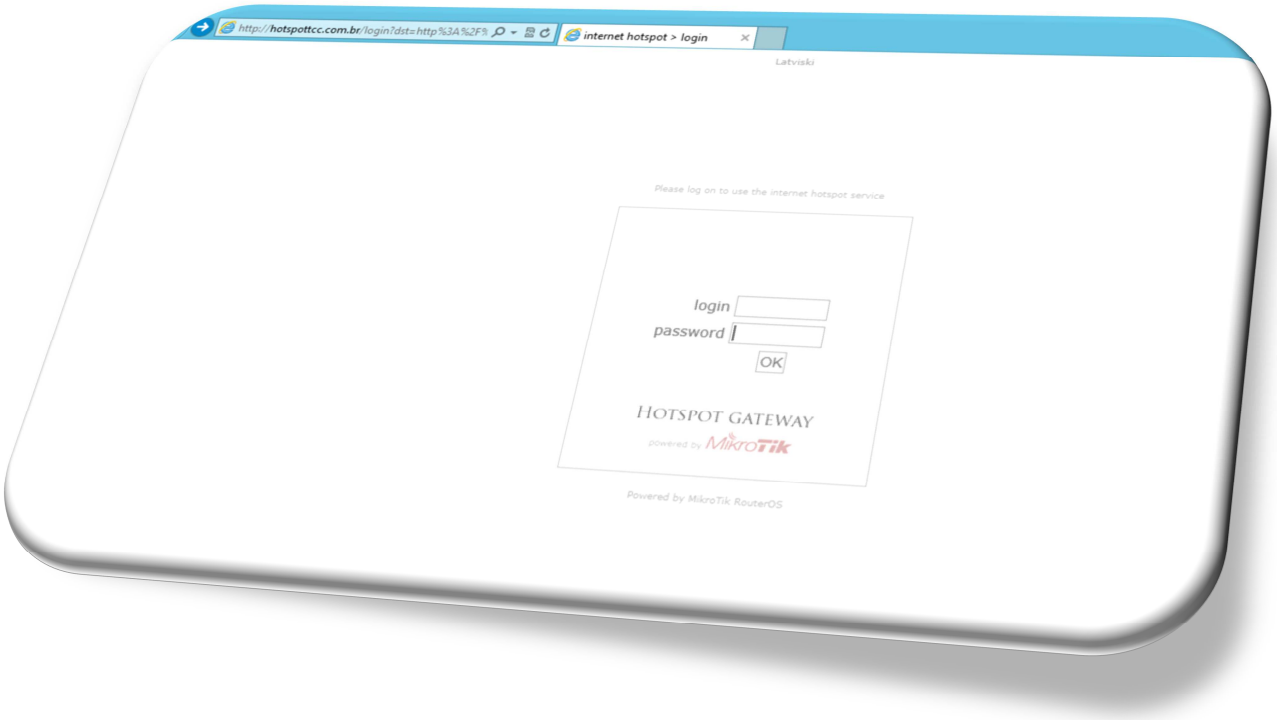
MANUAL PARA A CRIAÇÃO E CONFIGURAÇÃO DE UM SERVIDOR HOTSPOT NO SISTEMA OPERACIONAL ROUTEROS UTILIZANDO UMA ROUTERBOARD MIKROTIK



G U I L H E R M E L E V Y

GUARAPUAVA / PARANÁ

SETEMBRO / 2015

SUMÁRIO

ÍNDICE DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ADD	Addiction
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DST	Destination
IP	Internet Protocol
LAN	Local Architecture Network
MAC	Media Access Control
NAT	Network Address Translation
TCP	Transmission Control Protocol
SRC	Source
WIFI	Wireless Fidelity

1. OBJETIVO DO MANUAL

O principal objetivo deste manual é orientar o administrador da rede na implementação de um servidor hotspot utilizando uma Routerboard RB750 conforme a Imagem01, com o sistema operacional RouterOS da empresa Mikrotik.

Imagem 1: Routerboard RB750

Esse manual traz o roteiro detalhado para a configuração das interfaces, criação das redes, configuração de Web Proxy, configuração de firewall, criação e configuração do servidor hotspot e usuários, podendo ser utilizado também em outros modelos de Routerboards Mikrotik ou no sistema operacional RouterOS instalado em um microcomputador.

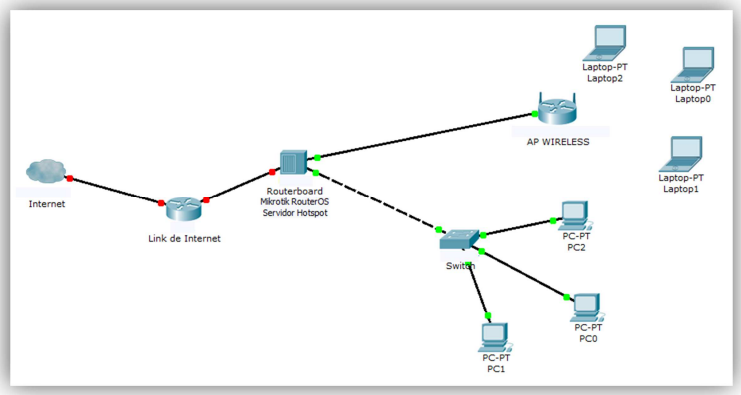


Imagem 2: Rede após a instalação do servidor hotspot

Conforme a representação da Imagem02 a Routerboard deve ser instalada entre o uplink de internet e os dispositivos de distribuição da internet para a rede local.

2.PRIMEIRO ACESSO E CONFIGURAÇÃO INICIAL

Para a criação das regras e acesso aos menus de configuração utilizaremos o programa Winbox na sua versão 3.0, que pode ser baixado gratuitamente na internet conforme o link http://download2.mikrotik.com/routeros/winbox/3.0rc12/winbox.exe.

Iremos conectar nosso computador à porta número 5 da Routerboard.

Abaixo, na imagem03 podemos visualizar a tela de login do programa Winbox para nos conectar ao sistema operacional RouterOS da Routerboard. Como a Routerboard ainda não possui configuração de rede devemos nos conectar pelo seu respectivo endereço MAC. O usuário padrão é admin e o campo senha não deverá ser preenchido conforme especificação padrão do equipamento.

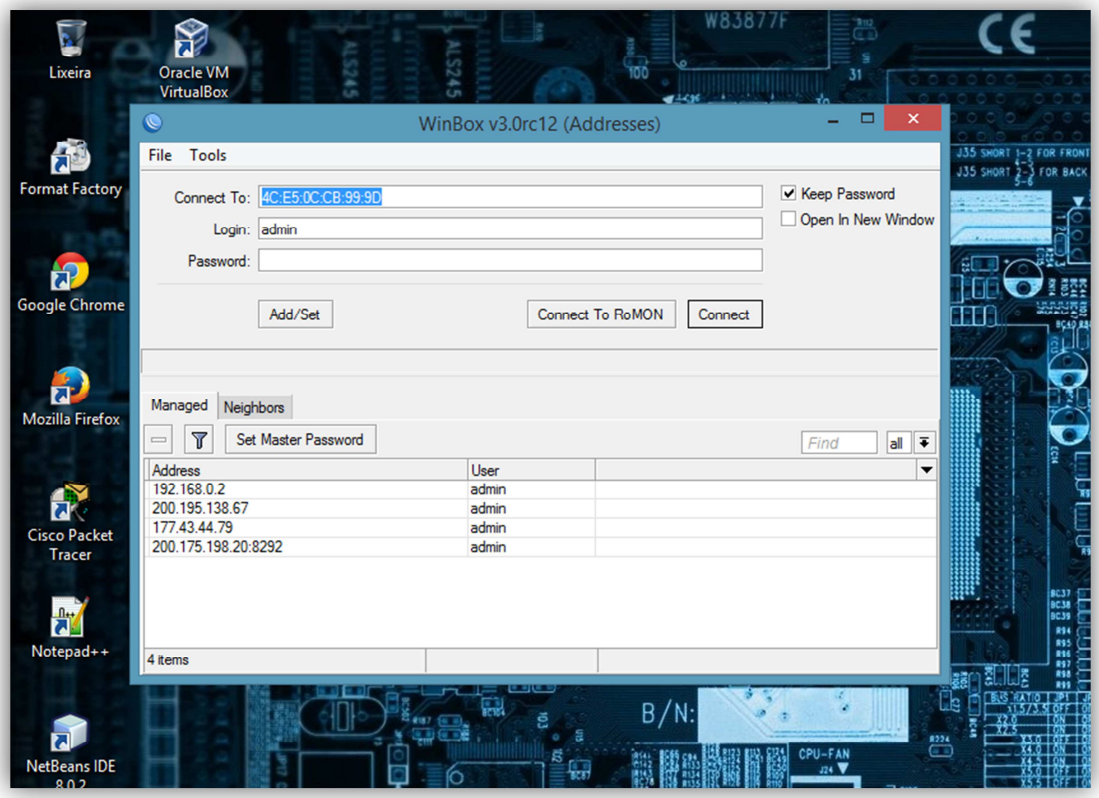


Imagem 3: Tela de login do aplicativo Winbox

Na imagem abaixo podemos visualizar a tela inicial após o acesso com o login e senha realizado pelo administrador no RouterOS com o programa Winbox. Nos próximos itens as imagens serão redimensionadas e focadas nos menus e submenus para uma melhor visualização e entendimento do conteúdo.

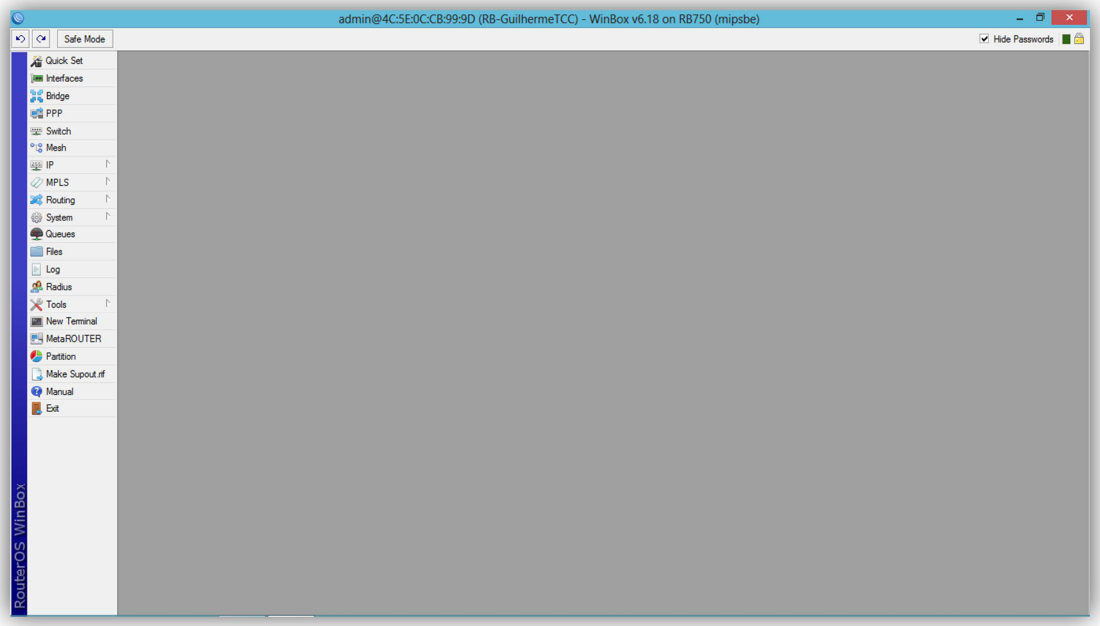


Imagem 4: Tela inicial do Winbox

Para iniciar os procedimentos de configuração devemos identificar nossa Routerboard a fim de personalizá-la em utilizações futuras, tal como identificação de arquivo de backup.

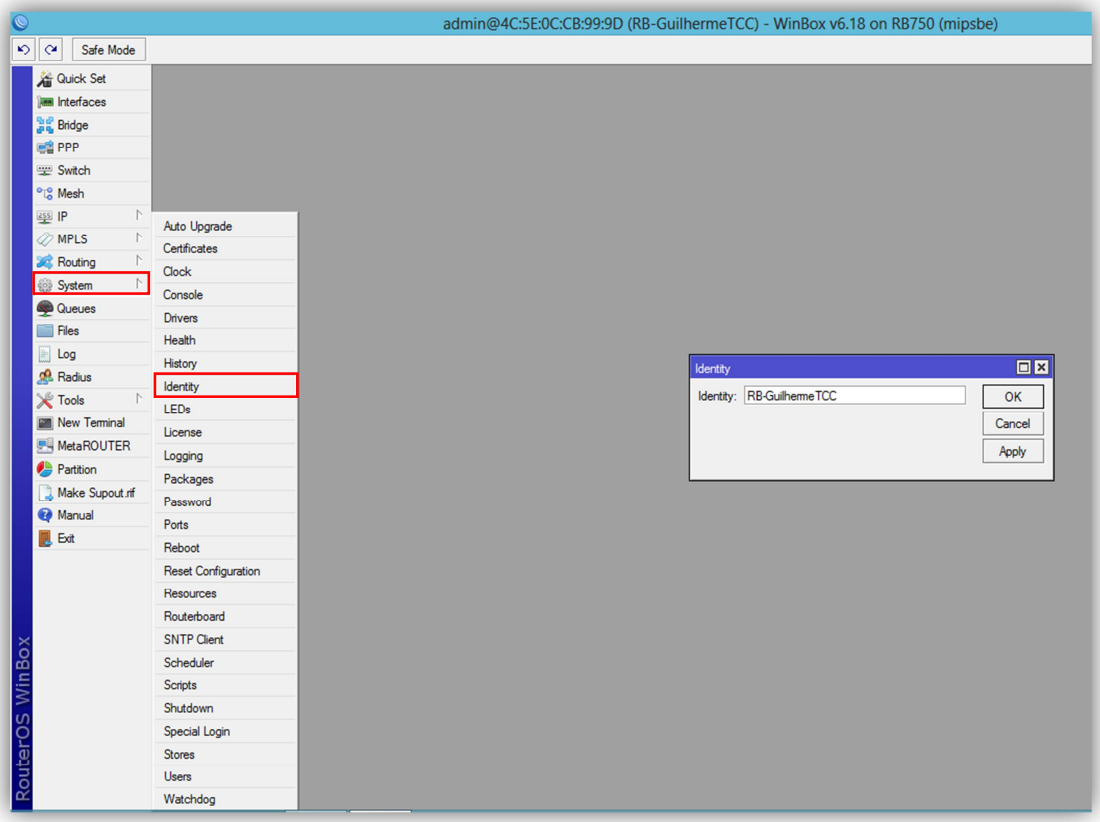


Imagem 5: Identificação da Routerboard

Seguindo a ideia de organizar a Routerboard para uma correta geração dos relatórios e arquivos de backup quando necessário e para garantir um funcionamento sem erros de interpretação das regras devemos fazer as configurações de hora, data e fuso horário.

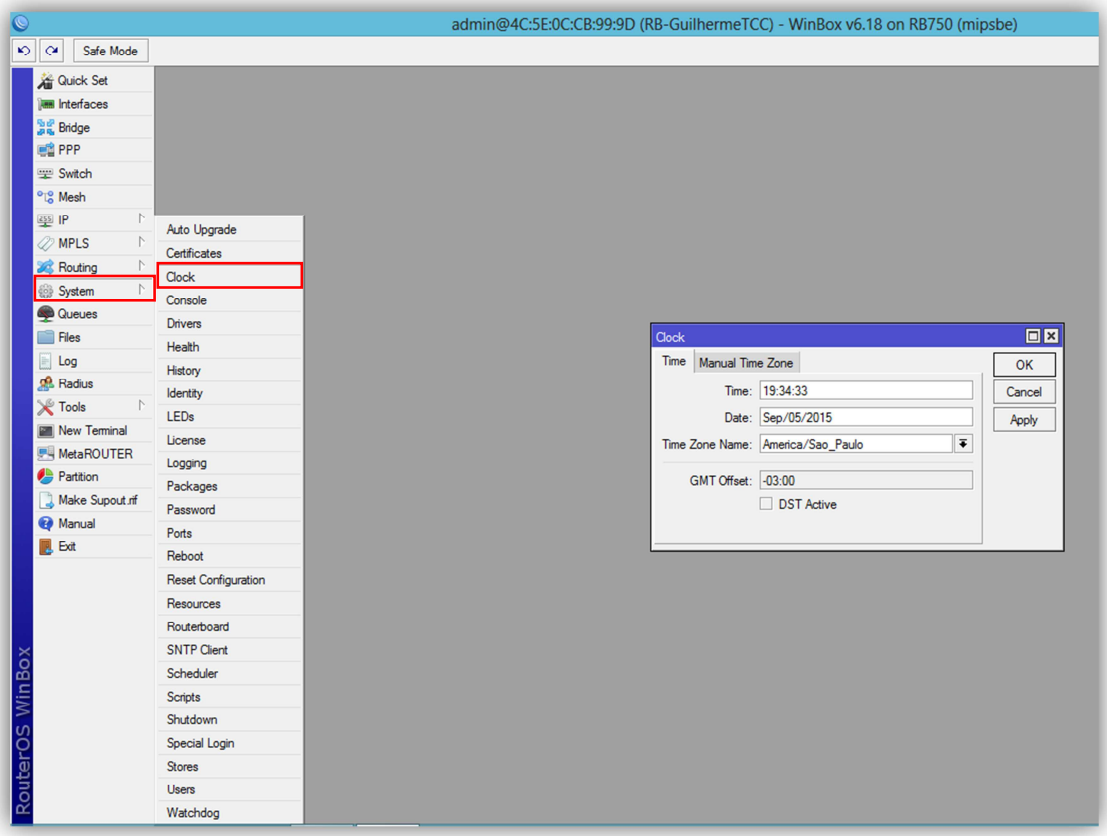


Imagem 6: Correção de hora/data

3. IDENTIFICAÇÃO E PERSONALIZAÇÃO DAS INTERFACES

Na imagem abaixo podemos visualizar a tela das interfaces disponíveis para a utilização no RouterOS. Entraremos no Menu: **Interfaces**

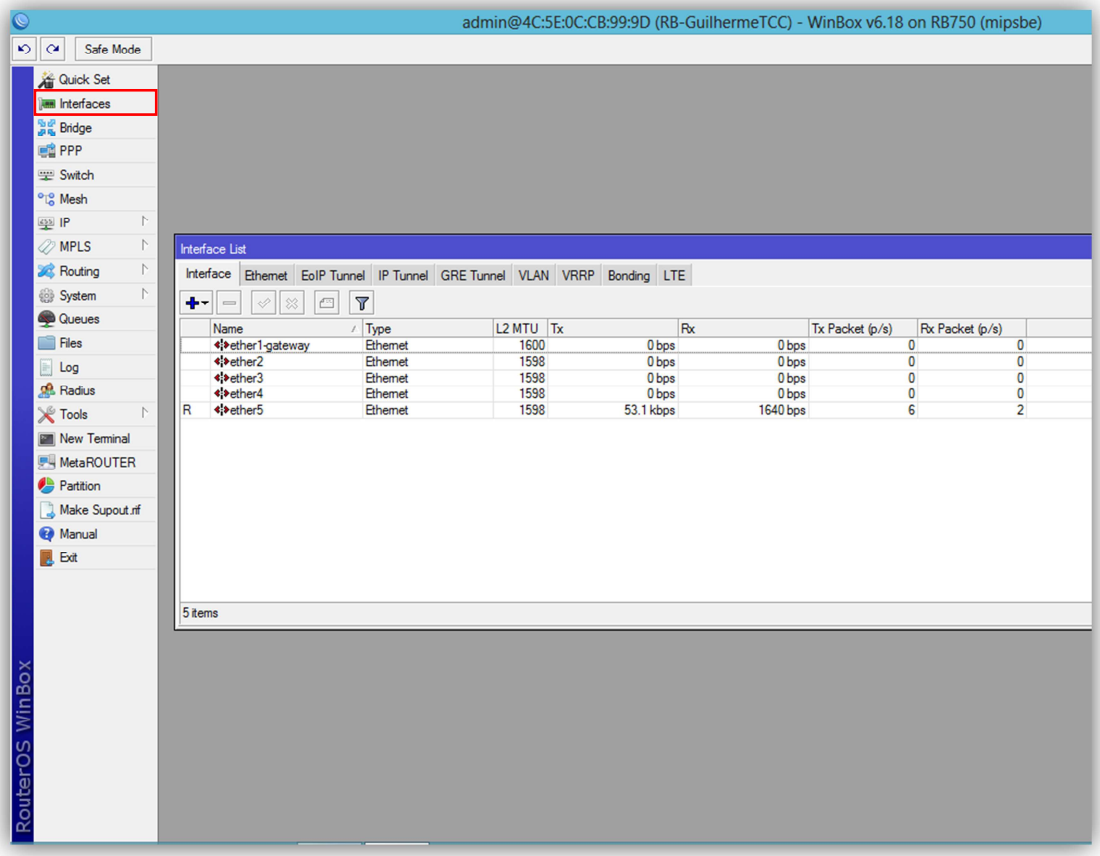


Imagem 7: Interfaces da Routerboard

3.1. RENOMEANDO A ETHER1 (UPLINK)

Escolheremos primeiramente a interface ether1-gateway (porta1) dando dois cliques para que nos seja mostrada a janela com as configurações padrão da porta. Na opção “Name” colocaremos o nome “Uplink” para identificá-la como a porta em que conectaremos o link de entrada da internet, na configuração utilizada nesse manual será disponibilizada somente uma porta para o uplink de internet.

Deixaremos a opção ARP como enable para que os pacotes de reconhecimento da rede que seja conectada na porta possam ser utilizados por essa interface, na opção de Bandwidth que limita o fluxo de dados na interface deixaremos unlimited, ou seja, sem limite de banda de tráfego de dados nessa interface. Os outros campos deixaremos com os valores padrão do RouterOS e clicaremos em OK.

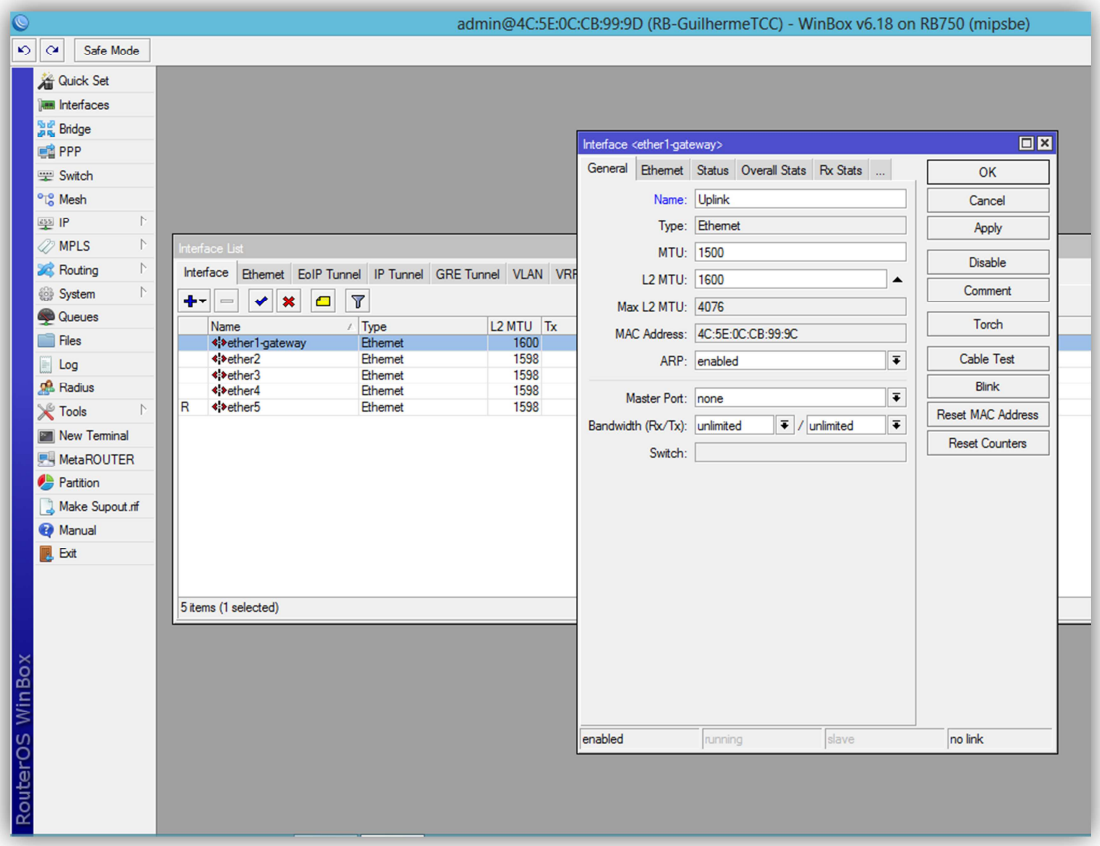


Imagem 8: Nomeação da interface ether1

3.2. RENOMEANDO A ETHER5 (OUTSWITCH)

Assim como na ether1 alteraremos somente o nome da ether5 (porta5) para OutSwitch, essa interface será responsável por transmitir os dados já tratados pela Routerboard para um microcomputador ou para os dispositivos de rede responsáveis pela distribuição da rede, em nosso caso, um Acess Point Wireless e um Swtich ethernet.

Na imagem abaixo podemos visualizar como ficará a tela de configuração da ether5 após as alterações.

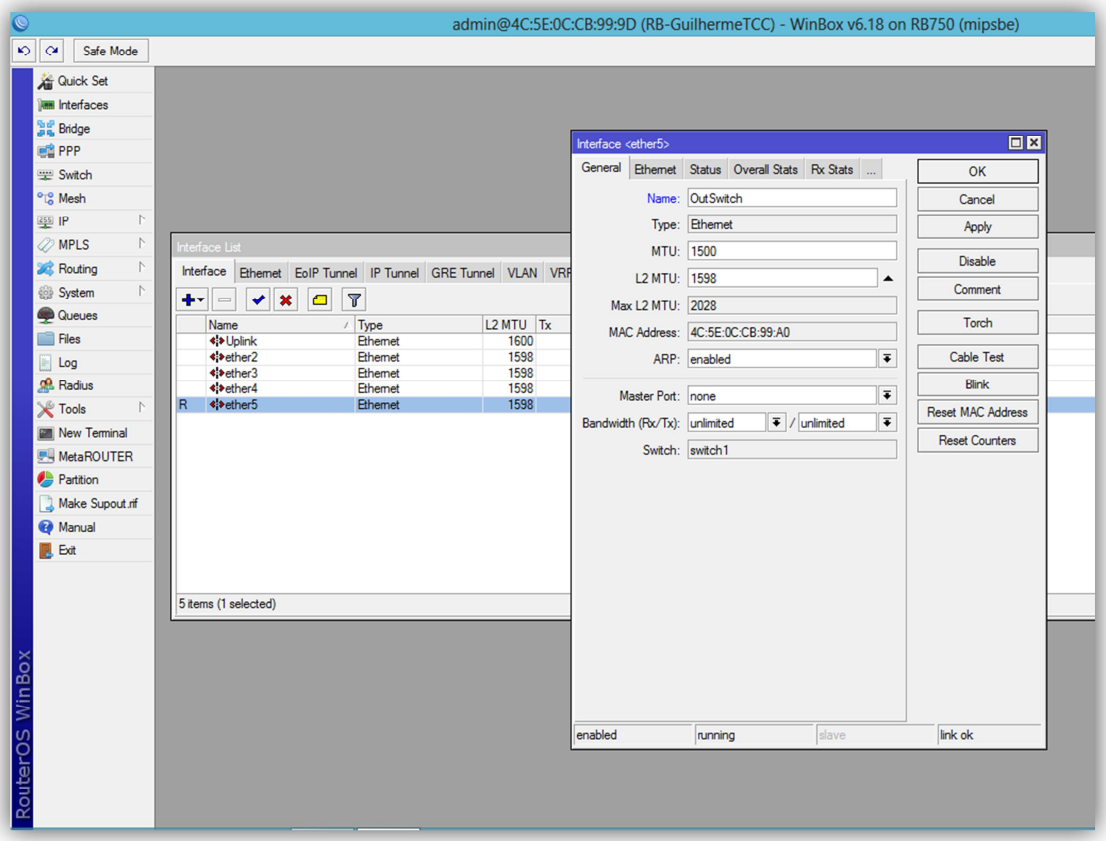


Imagem 9: Nomeação da interface ether5

3.3. FINALIZANDO A PERSONALIZAÇÃO DAS INTERFACES

Na imagem a seguir podemos visualizar a listagem de interfaces após à sua personalização e identificação. Podemos reparar ainda na letra R ao lado da interface OutSwitch que significa “Running”, ou seja, a interface já reconheceu o cabo conectado em sua porta e já está em funcionamento.

Obs: Lembrando que o cabo do Uplink de internet ainda não deve estar conectado na porta 5 da routerboard, conectaremos o cabo somente após a criação do DHCP Client, tópico abordado nos capítulos a seguir.

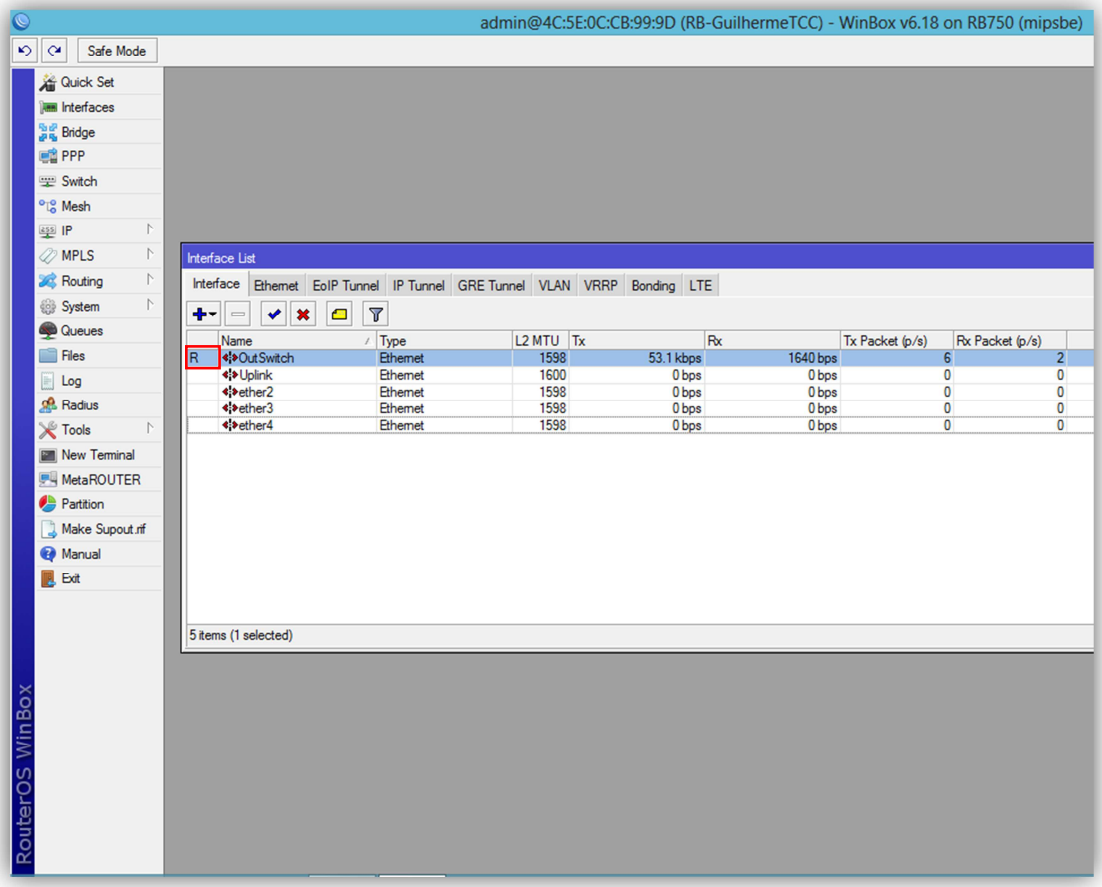


Imagem 10: Tela das interfaces após as alterações

4. ADDRESS LIST

Agora iniciaremos a configuração dos endereços de rede estáticos que poderão trafegar dados dentro de nossa Routerboard. Entraremos no Menu: **IP=>Addresses** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

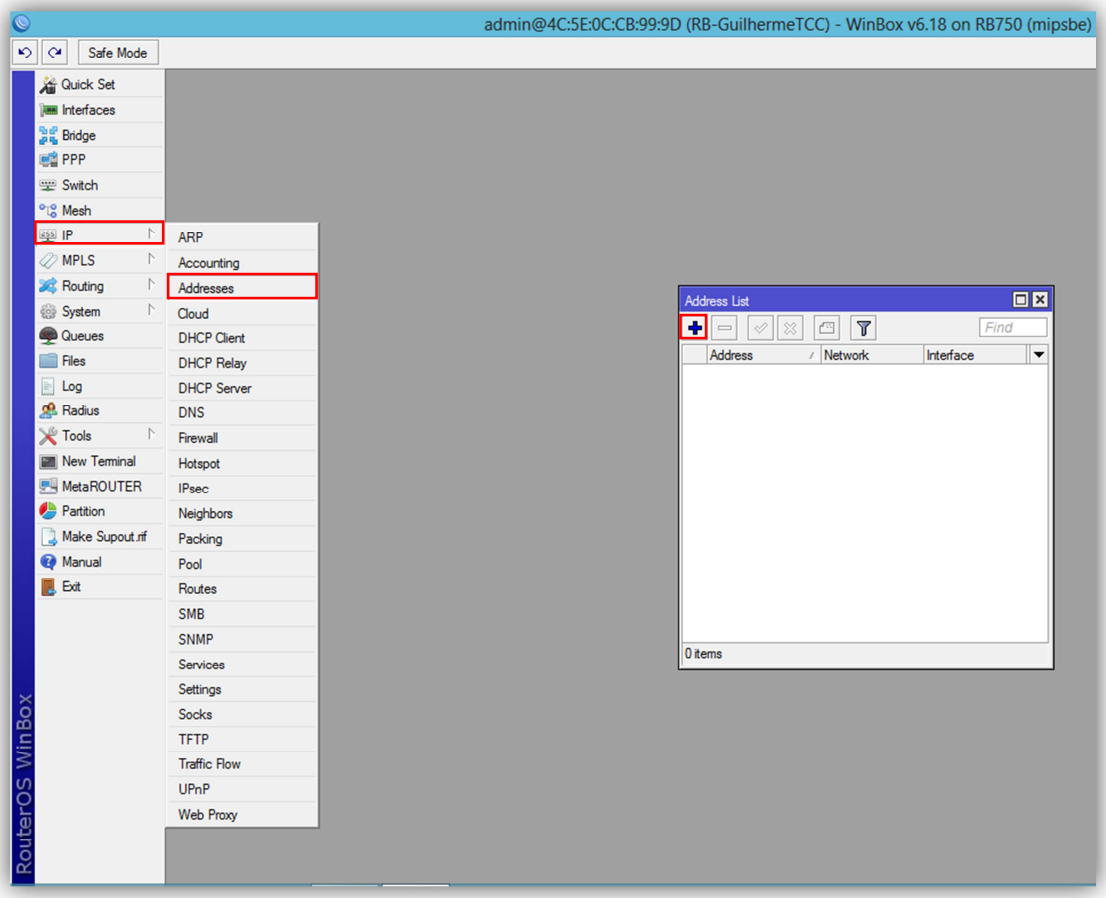


Imagem 11: Tela de configuração da Address List

4.1. ADICIONANDO UM NOVO ADDRESS ESTÁTICO

Antes de iniciar as configurações específicas de cada função no RouterOS precisamos definir quais são os endereços estáticos que poderão trafegar dados dentro de nossa Routerboard. Escolheremos a classe 192.168.10.0 para a criação de nosso servidor hotspot, portanto na opção **Address**, que será o enderenço IP que nossa Routerboard poderá ser acessada através do Winbox colocaremos 192.168.10.1/24, na opção **Network** colocaremos o endereço da rede escolhida 192.168.10.0 e no campo **Interface** escolheremos por qual delas essa rede estará acessível, em nosso caso a interface **OutSwitch** e depois clicaremos em **OK**. Nesse ponto já começamos a entender a importância da correta personalização prévia das interfaces, para que na hora das configurações dos vínculos das interfaces com os addresses não ocorra nenhuma troca e dificulte a finalização da implantação do servidor hotspot.

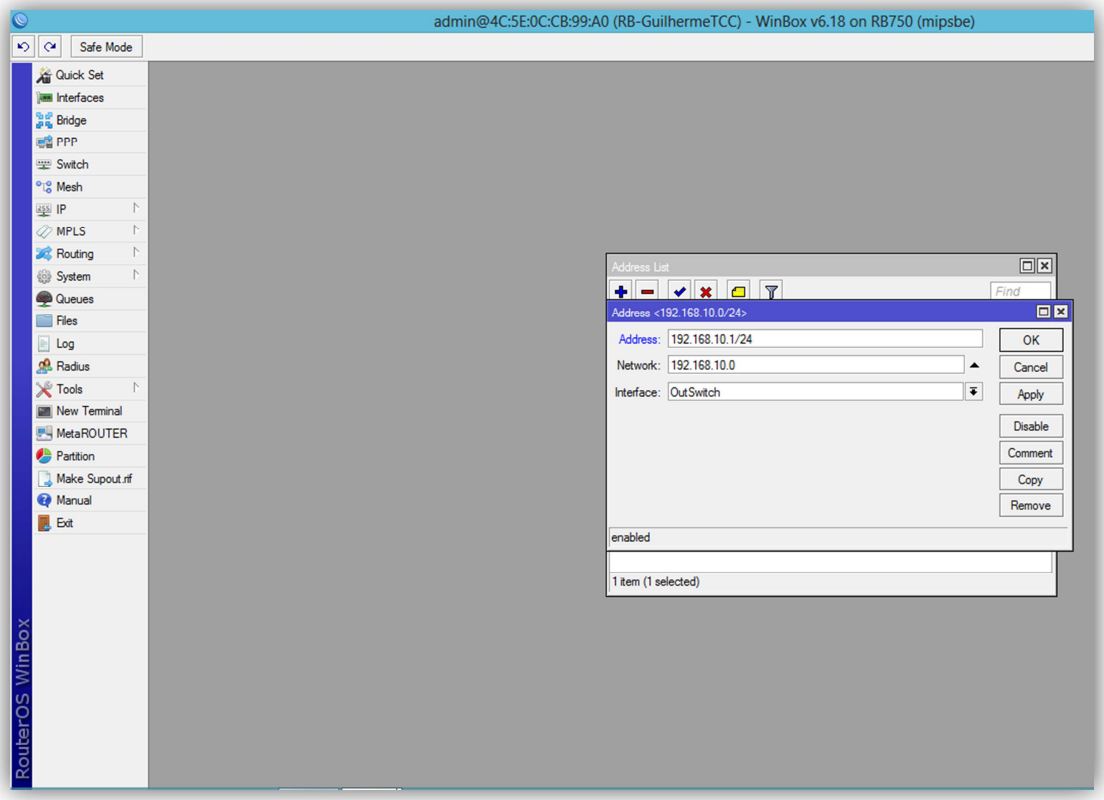


Imagem 12: Tela de inclusão de um Address estático

Na imagem abaixo podemos visualizar como ficará a Address List após a inclusão da nossa rede principal.

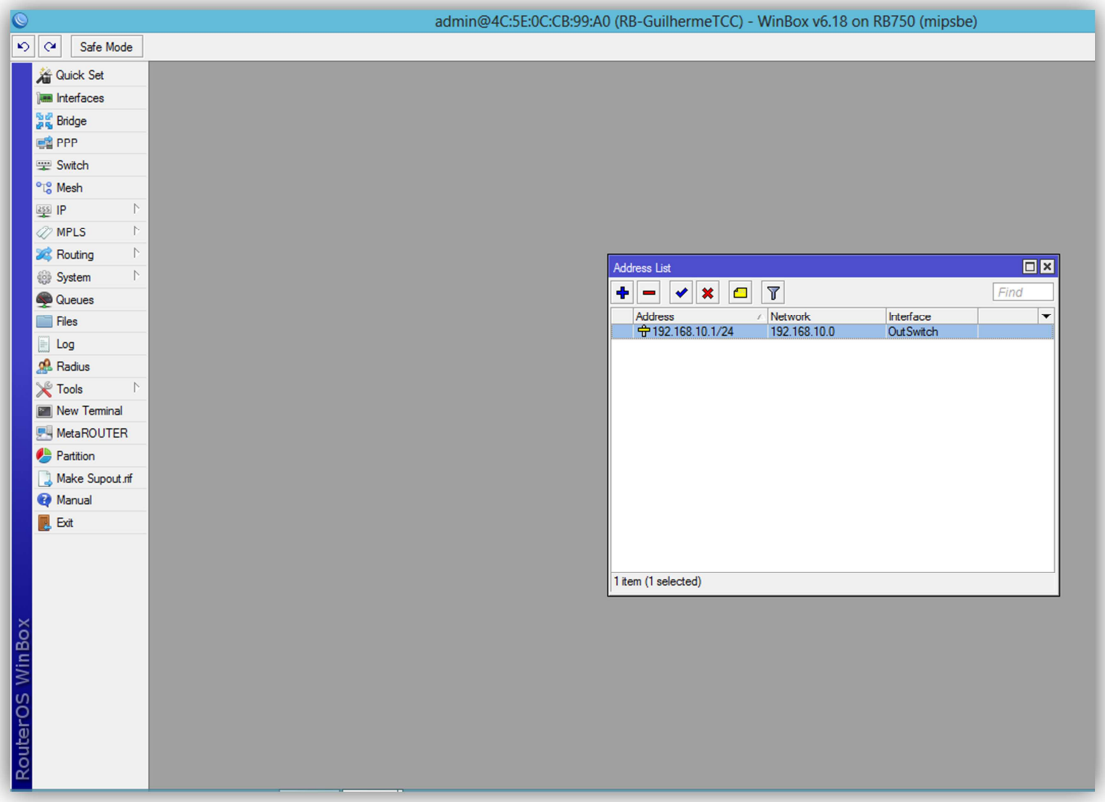


Imagem 13: Finalizando a inclusão de um Address estático

5. IP POOL

Agora iremos configurar um POOL de endereços de ip para nossa rede, o IP POOL é o escopo do DHCP Server, ou seja, é uma faixa de endereços de ip que o DHCP Server poderá conceder aos clientes.

Agora iniciaremos a inclusão de um POOL de endereços de ip em nossa Routerboard. Entraremos no Menu: **IP=>IP POOL** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

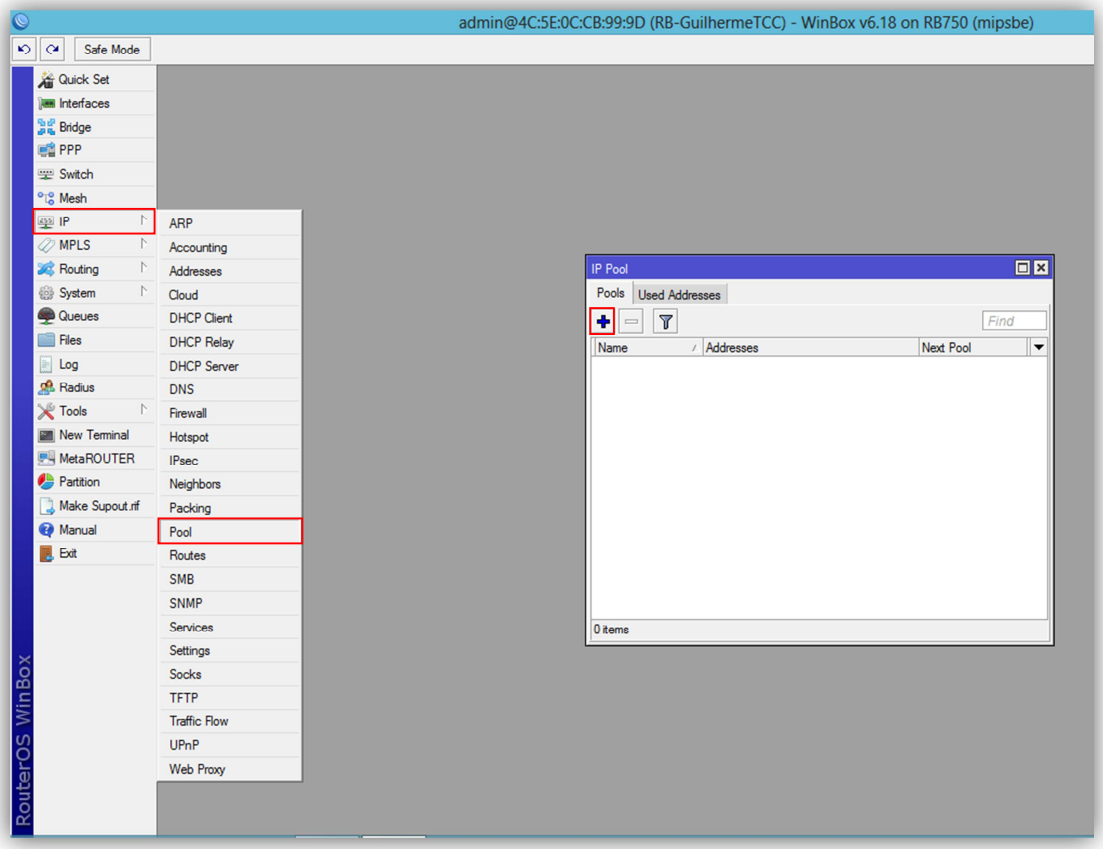


Imagem 14: Tela inicial de configuração do IP Pool

5.1. ADICIONANDO UM NOVO IP POOL

Na janela “**New IP POOL**” colocaremos no campo **Name** o nome de “**PoolHSP**” para o novo Pool de endereços de ip, no campo **Addresses** colocaremos a faixa de ip que será disponibilizada pelo DHCP Server, nesse caso utilizaremos a faixa de 192.168.10.5-192.168.10.254, portanto serão 250 endereços de ip utilizáveis pelo no DHCP Server para os microcomputadores ou dispositivos conectados a ele.

Na opção **Next Pool** deixaremos none, essa opção é utilizada quando necessitamos de uma quantidade maior que 253 endereços de ip para o DHCP Server conceder aos microcomputadores ou dispositivos, então se temos dois IP POOL criados colocamos nessa opção esse segundo IP POOL criado e ao acabar os endereços do primeiro ele automaticamente começará a conceder os endereços de ip do segundo IP POOL existente.

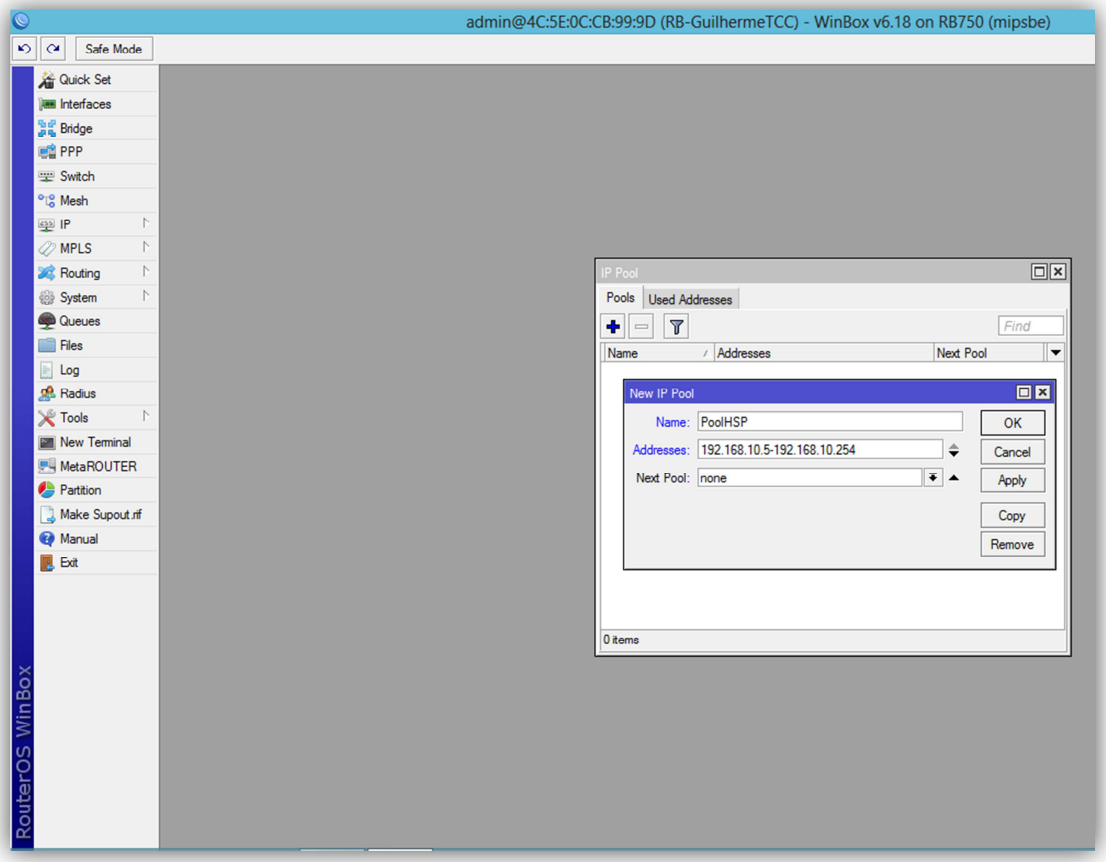


Imagem 15: Tela de inclusão de um novo IP Pool

Na imagem abaixo podemos visualizar como ficará a tela inicial do IP POOL após a inclusão do nosso novo IP POOL.

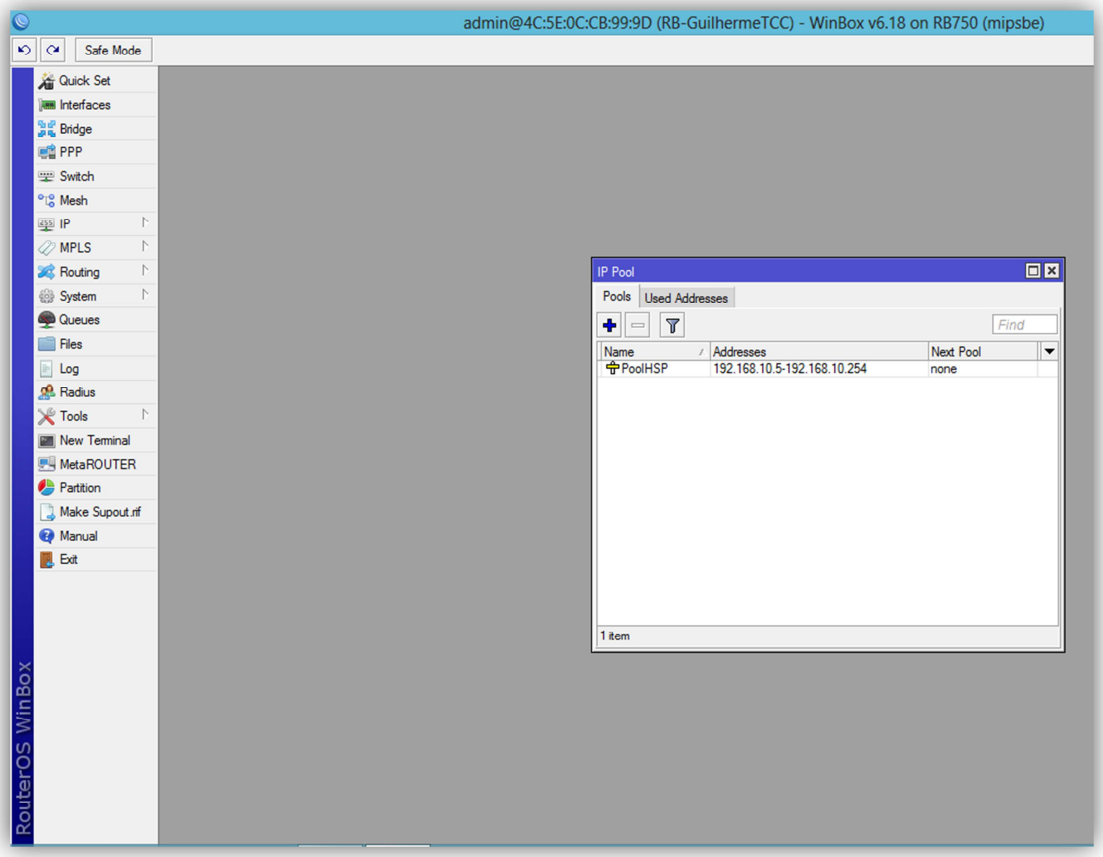


Imagem 16: Finalizando a inclusão de um IP POOL

6. DHCP SERVER

A imagem abaixo nos mostra os servidores DHCP existentes em nossa routerboard, o protocolo DHCP é o serviço responsável por uma configuração dinâmica dos microcomputadores ou dispositivos conectados a ele, incluindo atribuição de IP, máscaras de sub-rede, default gateway e servidores DNS.

Agora iniciaremos a inclusão de um servidor DHCP em nossa Routerboard. Entraremos no Menu: **IP=>DHCP Server** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

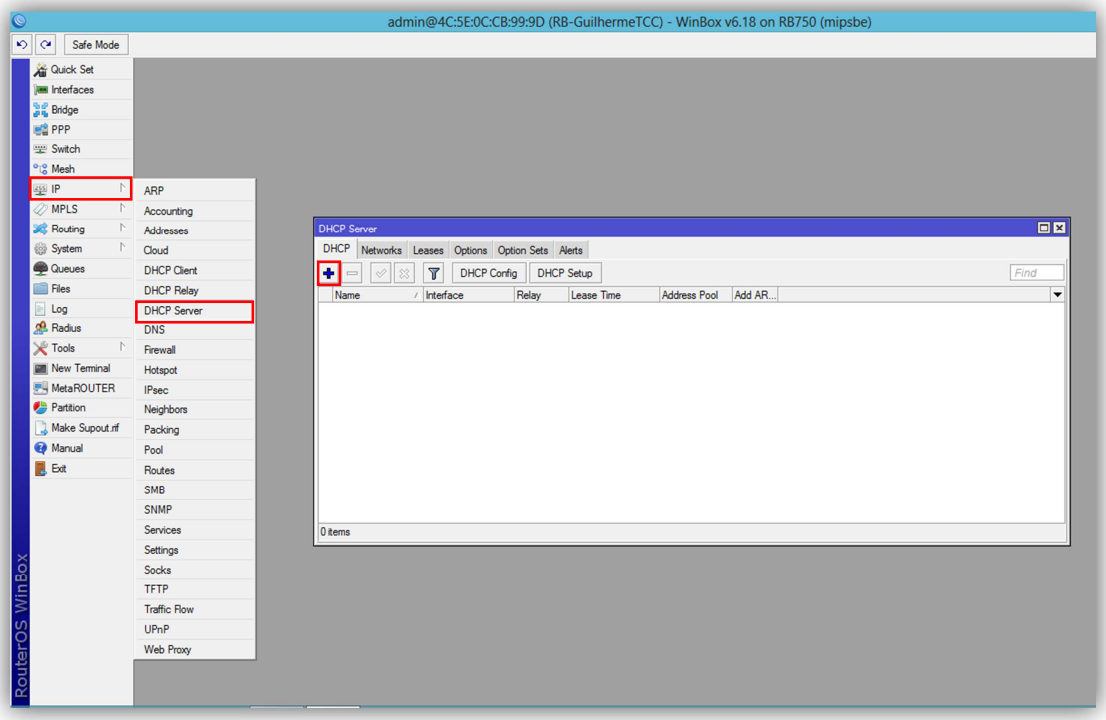


Imagem 17: Tela inicial de configuração do DHCP Server

6.1. ADICIONANDO UM NOVO DHCP SERVER

Na janela “**New DHCP Server**” iniciaremos a configuração dando um nome ao nosso servidor, sempre lembrando que é uma boa prática colocarmos nomes que facilitem a identificação do serviço nas próximas etapas, no caso de você possuir mais de um servidor DHCP configurado nesse mesmo RouterOS.

Nesse caso colocaremos no campo **Name** o nome de “**ServerHSP**” para o novo servidor, no campo **Interface** selecionaremos a interface que será responsável por fornecer as configurações do DHCP aos microcomputadores e dispositivos conectados a ele, nesse caso a interface OutSwitch. No campo **Lease Time** colocaremos o tempo de 02:00:00 horas, o Lease Time é o tempo que o endereço de ip estará disponível para um endereço MAC após a primeira utilização desse ip por esse determinado MAC. No campo Address Pool selecionaremos o “**PoolHSP**” criado anteriormente. Nos demais campos deixaremos o padrão do RouterOS, como mostrado na imagem abaixo.

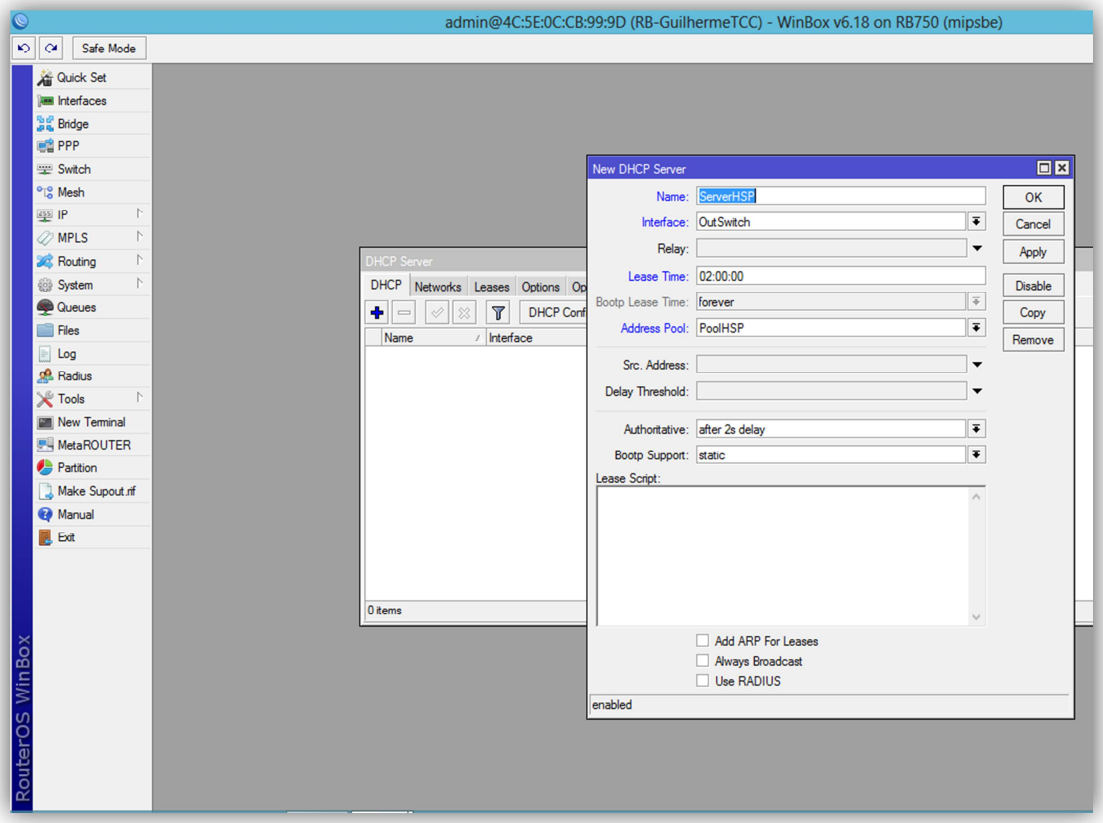


Imagem 18: Criando um novo DHCP Server

Na imagem abaixo podemos visualizar como ficará a tela inicial do DHCP Server após a inclusão do nosso novo servidor DHCP.

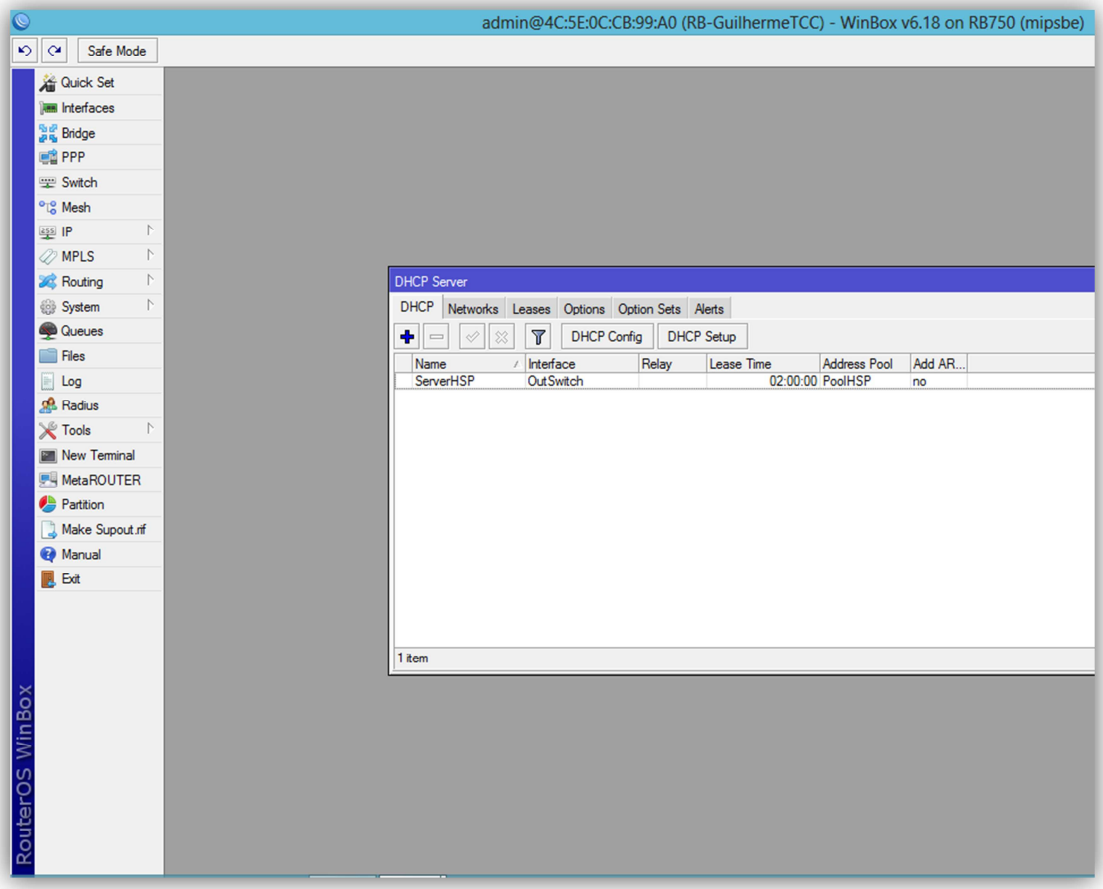


Imagem 19: Finalizando a inclusão de um DHCP server

6.2. DHCP Server => NETWORKS

Na opção **Networks** do Router iremos configurar os Gateways de nossas redes, na opção Networks também é possivel configurar servidores DNS individuais para cada rede, nós não faremos isso e será explicado o motivo no tópico **DHCP Client**.

Agora iniciaremos a configuração de um Networks. Entraremos no Menu: **IP=>DHCP Server** e clicaremos na guia **Networks,** selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

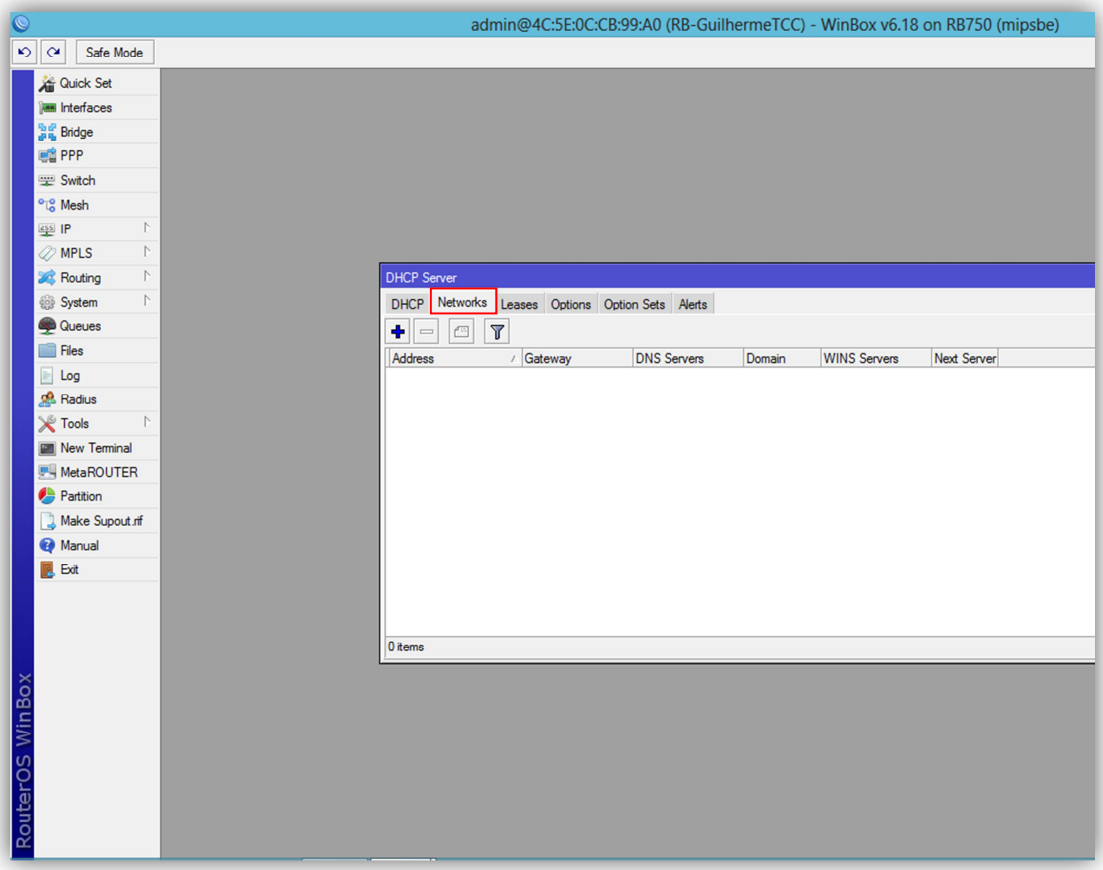


Imagem 20: Tela inicial de configuração Networks

6.2.1. ADICIONANDO UM NOVO NETWORKS

No campo **Address** colocaremos a classe de nossa rede que será utilizada seguida pela máscara de sub-rede, nesse caso 192.168.10.0/24 e no campo **Gateway** colocaremos o gateway de nossa classe, 192.168.10.1, os demais campos serão não serão alterados.

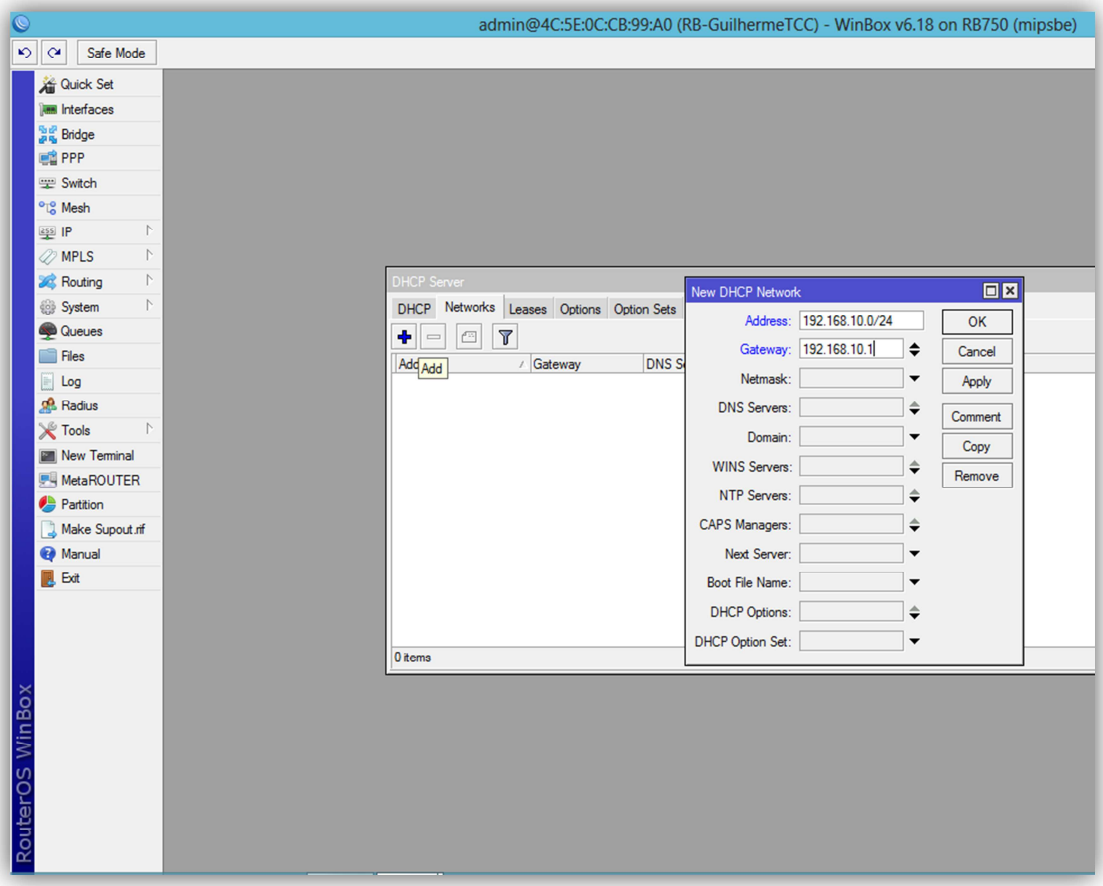


Imagem 21: Tela de inclusão de um novo Networks

Na imagem abaixo podemos visualizar como ficará a tela inicial do Networks após a inclusão do nosso novo Networks.

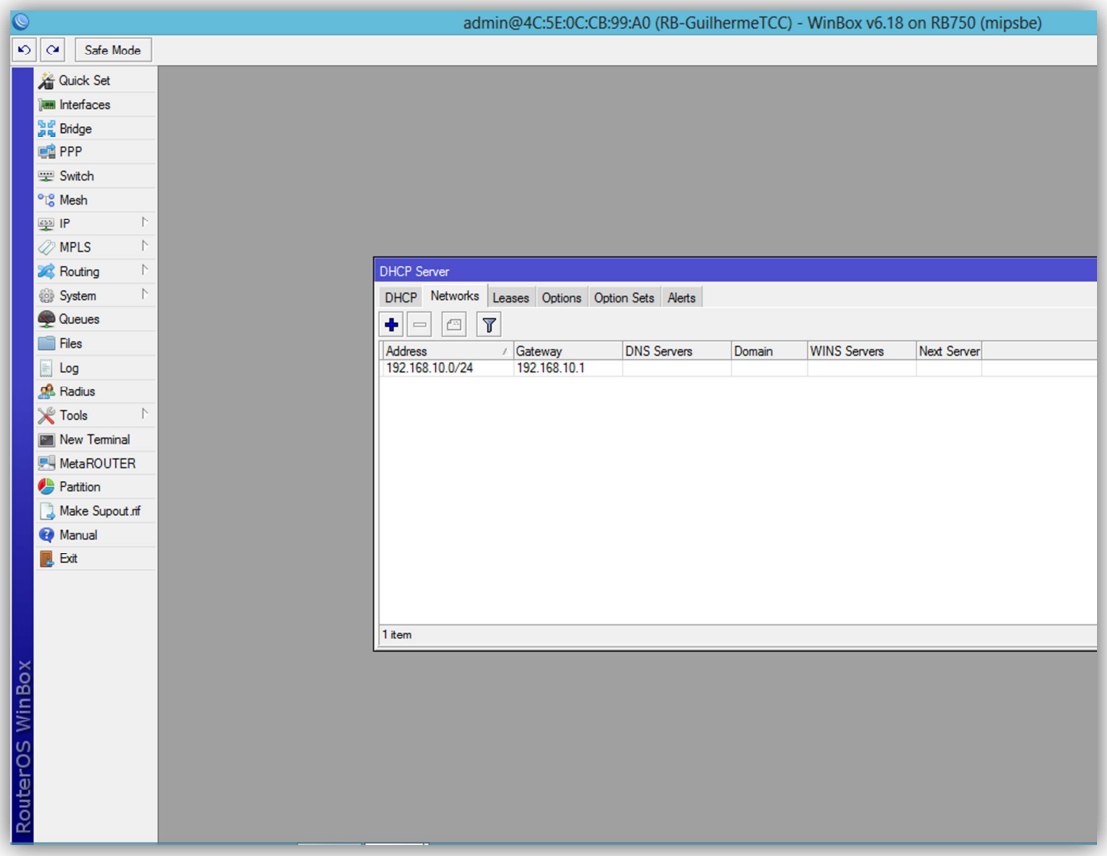


Imagem 22: Finalizando a inclusão de um Networks

Após essa etapa da configuração já é possível fazer o login no RouterOS pelo endereço de ip e não mais pelo endereço MAC, em nosso caso faremos o login pelo ip do gateway 192.168.10.1, como mostra a Imagem23.

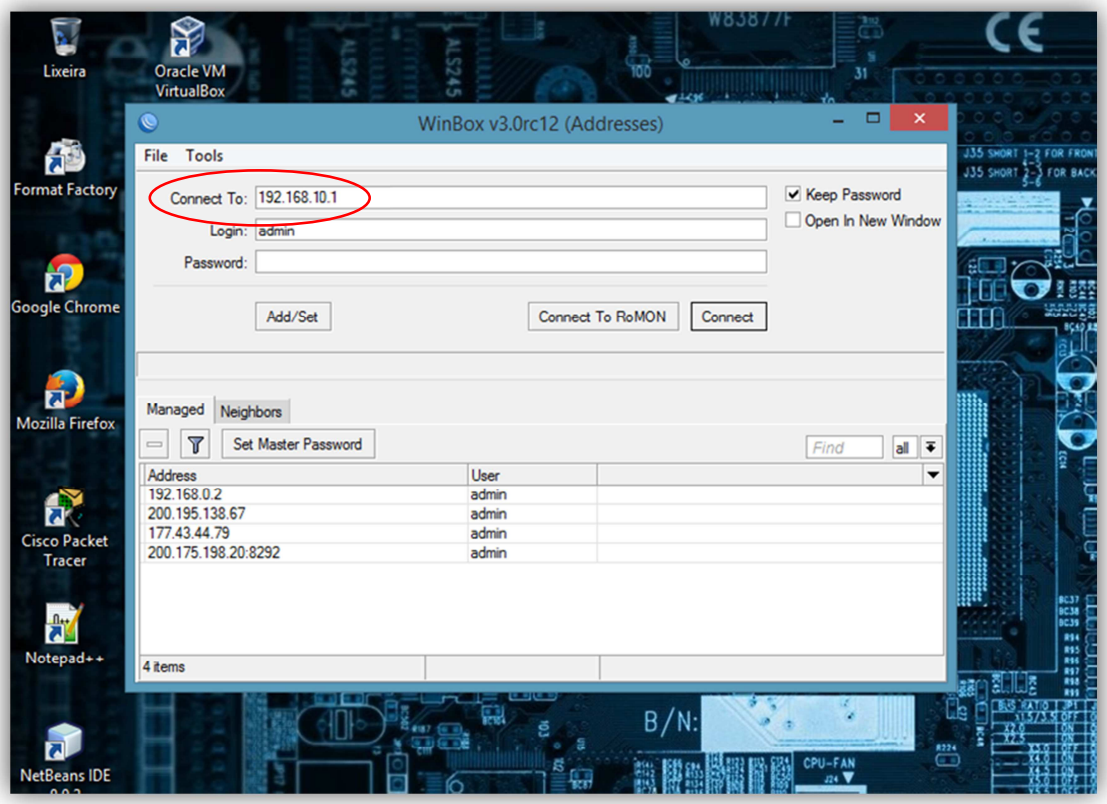


Imagem 23: Tela de login no RouterOS pelo endereço de ip

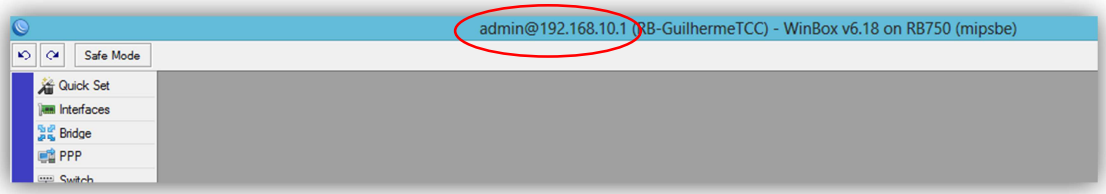


Imagem 24: Conectado no RouterOS pelo endereço de ip

7. DHCP CLIENT

A imagem abaixo nos mostra os clientes DHCP existentes em nossa Routerboard, o DHCP Client assim como o DHCP Server, possui uma configuração dinâmica dos dispositivos conectados a ele, mas por ser um cliente ele recebe dinamicamente as configurações de um servidor DHCP externo.

Agora iniciaremos a inclusão de um cliente DHCP em nossa Routerboard. Entraremos no Menu: **IP=>DHCP Client** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

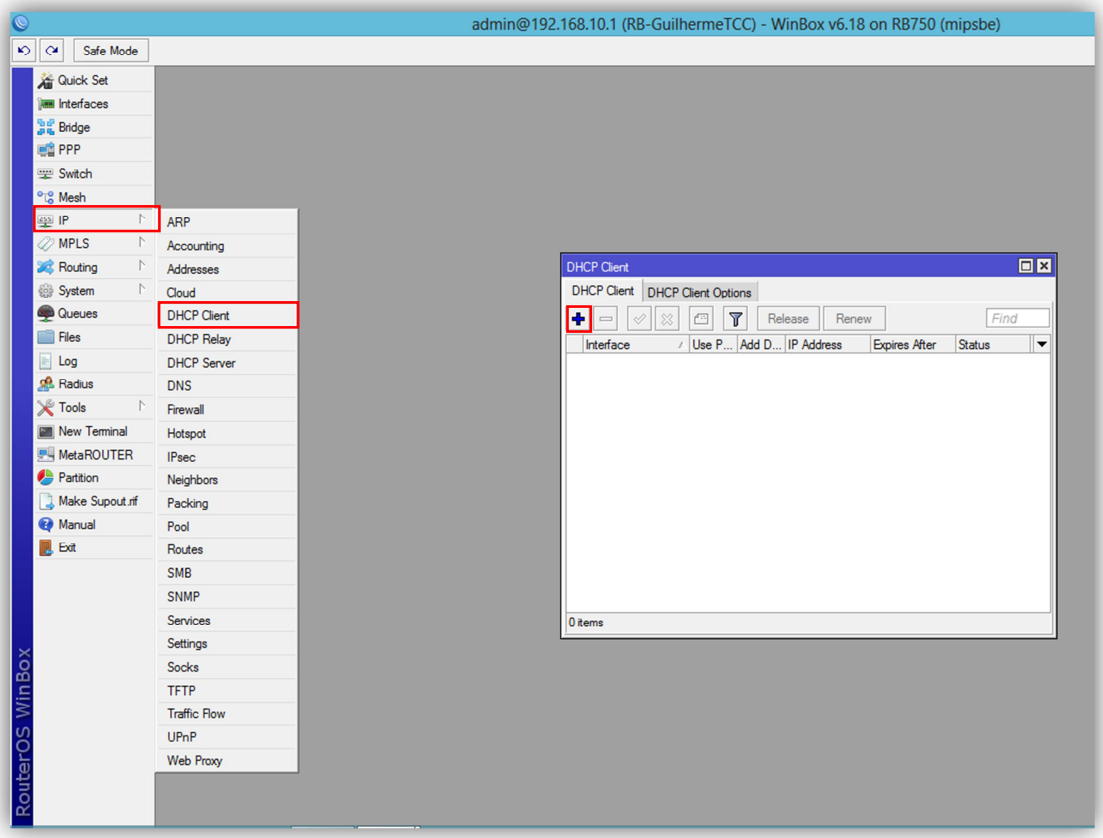


Imagem 25: Tela inicial de configuração do DHCP Client

7.1. ADICIONANDO UM NOVO DHCP CLIENT

Na inclusão de um DHCP Client faremos somente a escolha de qual interface será a responsável por receber as configurações dinâmicas, No campo **Interface** selecionaremos UpLink, portanto utilizaremos essa interface para receber o uplink de internet.

As opções **Use peer DNS** e **Use peer NTP** que fazem a sincronia com os servidores DNS e com os relógios dos dispositivos da rede do cliente respectivamente, deixaremos marcados.

Criando um DHCP Client desse modo faremos com que qualquer link de internet possa ser conectado a essa interface, desde que fornecido por um DHCP Server, os demais campos devem permanecer com a configuração padrão do RouterOS, como a figura abaixo.

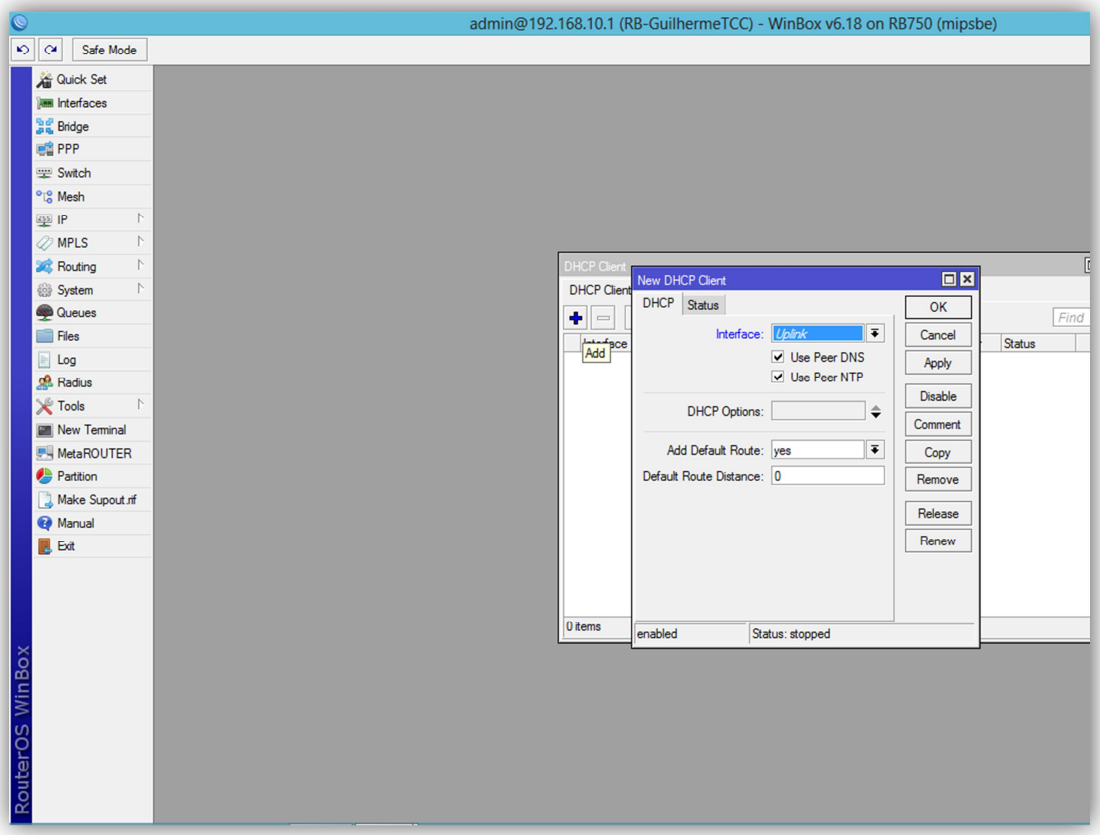


Imagem 26: Tela de inclusão de um DHCP Client

7.2. CONECTANDO UM UPLINK AO DHCP CLIENT

Como o protocolo DHCP trabalha dinamicamente, ao conectar o cabo na interface UpLink ele receberá as configurações de ip e DNS do DHCP Server que estiver fornecendo essas configurações e automaticamente configurará os servidores DNS de nossa rede, também criará na opção **Address List** os Address para que nossa rede reconheça e receba os dados da rede que o DHCP Client dinamicamente se configurou. Nas imagens abaixo mostramos como o DHCP se configura após a conexão do cabo do UpLink.

A Imagem28 mostrou que ele recebeu do servidor DHCP externo o endereço de ip 192.168.0.10/24.

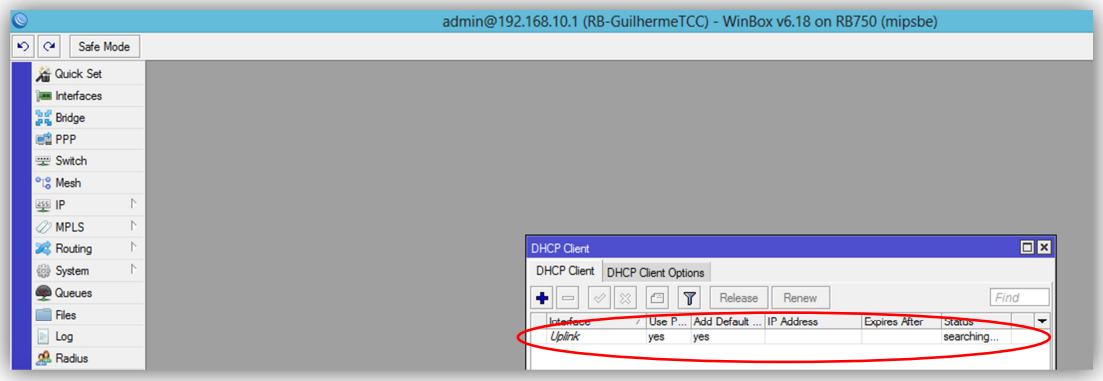


Imagem 27: DHCP Cliente antes da conexão do Uplink

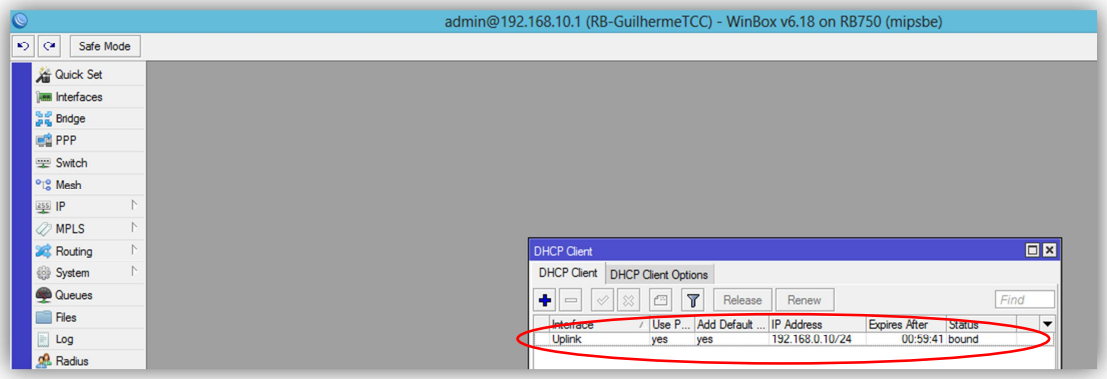


Imagem 28: DHCP Cliente após da conexão do Uplink

A Imagem29 mostrou que após ele receber o endereço de ip 192.168.0.10/24, ele dinamicamente cria o Address com sua Network e configura a interface responsável por ele, a letra **D** no inicio do Address significa **Dynamic**.

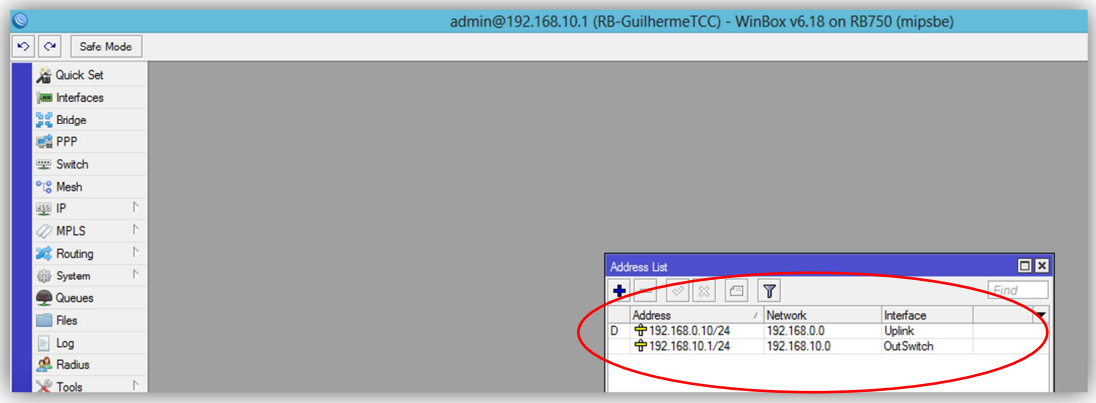


Imagem 29: Criação automática do Address

A Imagem30 mostrou que ele também configurou os servidores DNS automaticamente de acordo com as configurações do DHCP Server externo.

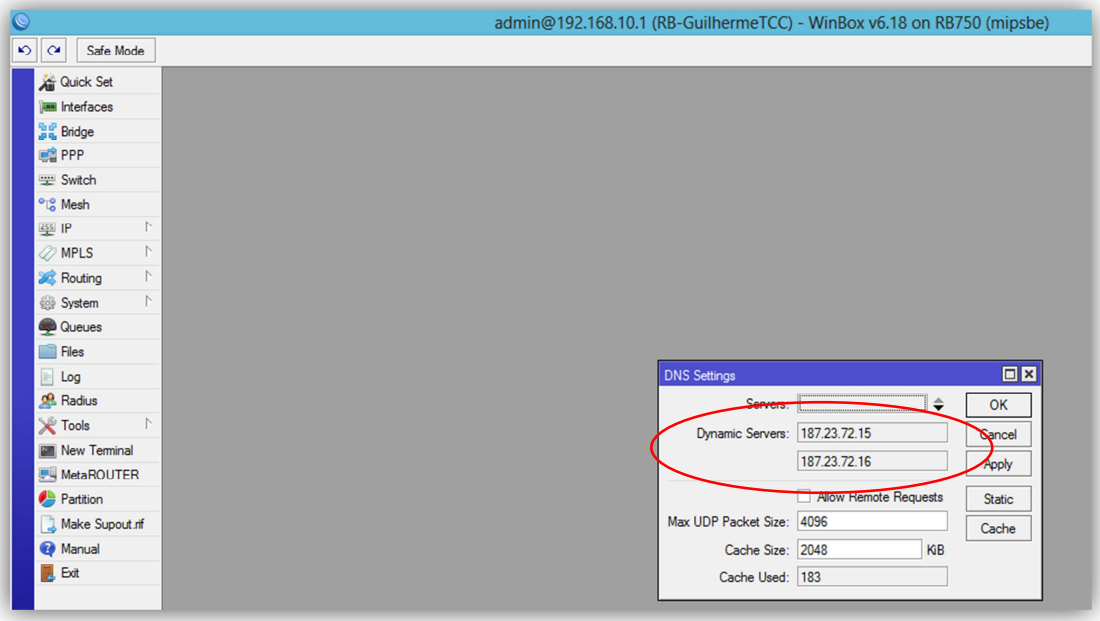


Imagem 30: Configuração automática dos servidores DNS

8. TESTANDO A CONEXÃO DA ROUTERBOARD

A conexão do uplink na Routerboard e o reconhecimento do uplink pelo DHCP Client faz com que a Routerboard esteja conectada na internet.

A imagem abaixo nos mostra uma janela do New Terminal com o teste de ping ao host 8.8.8.8 feito com sucesso.

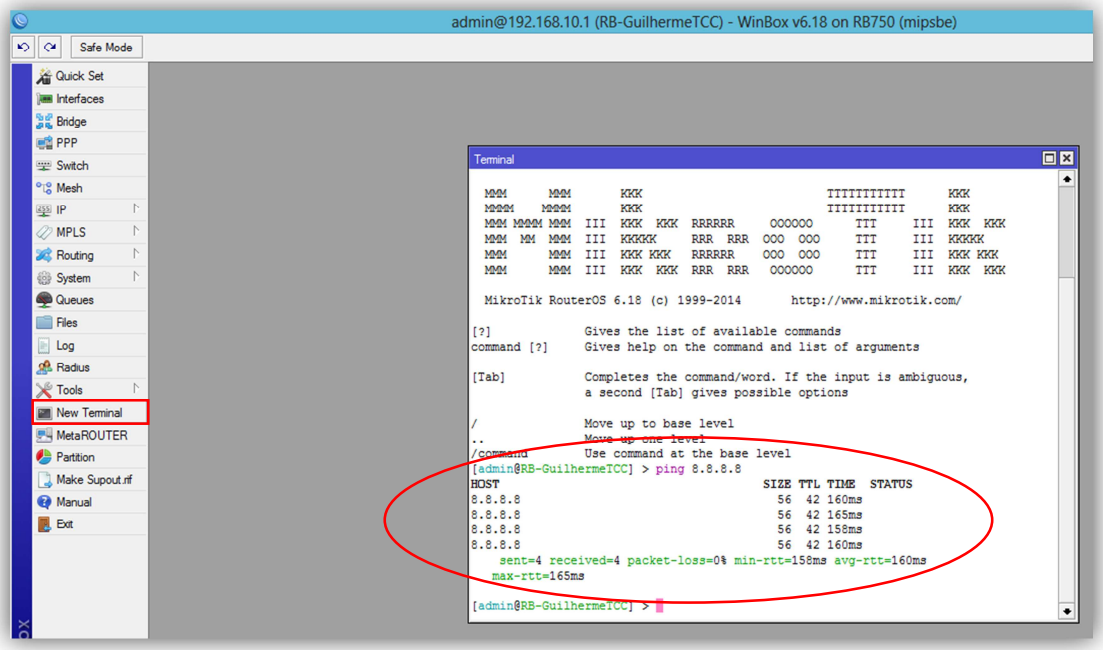


Imagem 31: Tela de teste de ping da Routerboard

9. FIREWALL

Após as configurações iniciais para fazermos a Routerboard navegar precisamos configurar o firewall para que a nossa rede tenha permissão do firewall para trafegar dados.

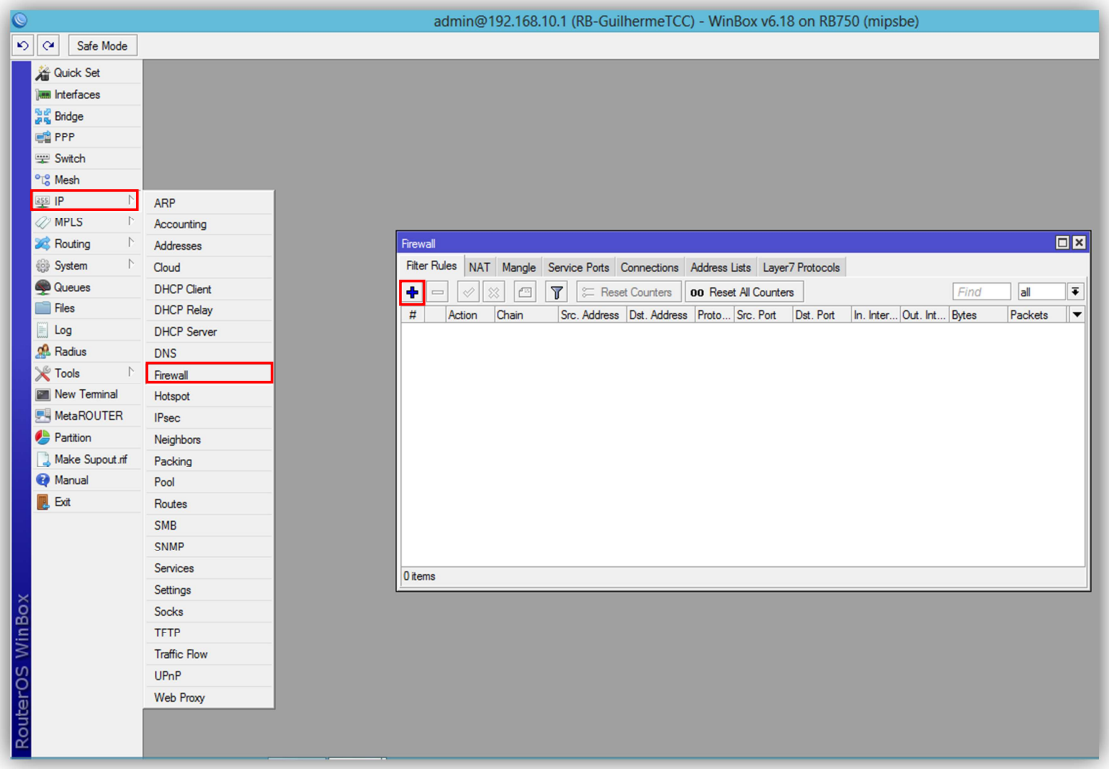


Imagem 32: Tela do Firewall

9.1. ADICIONANDO REGRAS DE FIREWALL

Agora iniciaremos a inclusão de uma regra no **Firewall** do RouterOS em nossa Routerboard. Entraremos no Menu: **IP=>Firewall** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida uma tela de **New Firewall Rule** como pode ser visualizado na imagem abaixo.

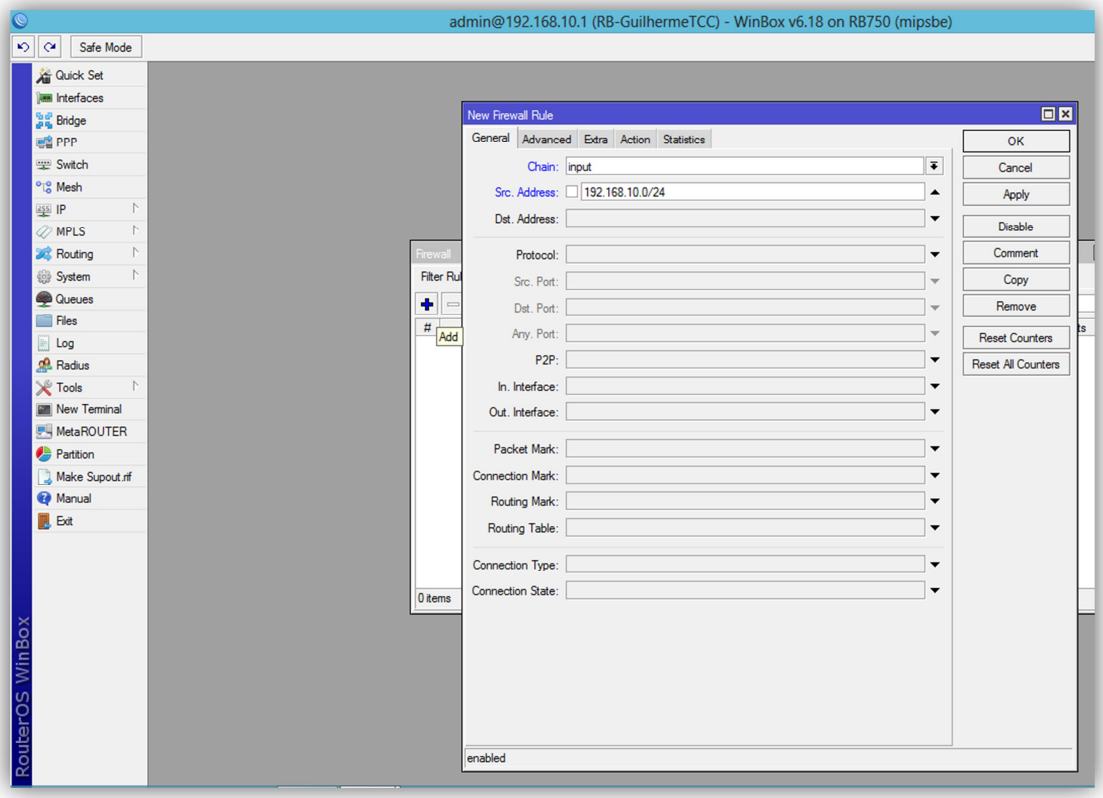


Imagem 33: Tela de criação de regras do Firewall

No campo **Chain** selecionaremos a opção input, ou seja, é todo o tráfego que vai para a Routerboard, no campo **Src.Address**colocaremos a classe e a máscara de sub-rede de nossa rede 192.168.10.0/24, devemos clicar na guia Action e no campo **Action** selecionar a opção accept e em seguida OK, como nos mostra a Imagem34.

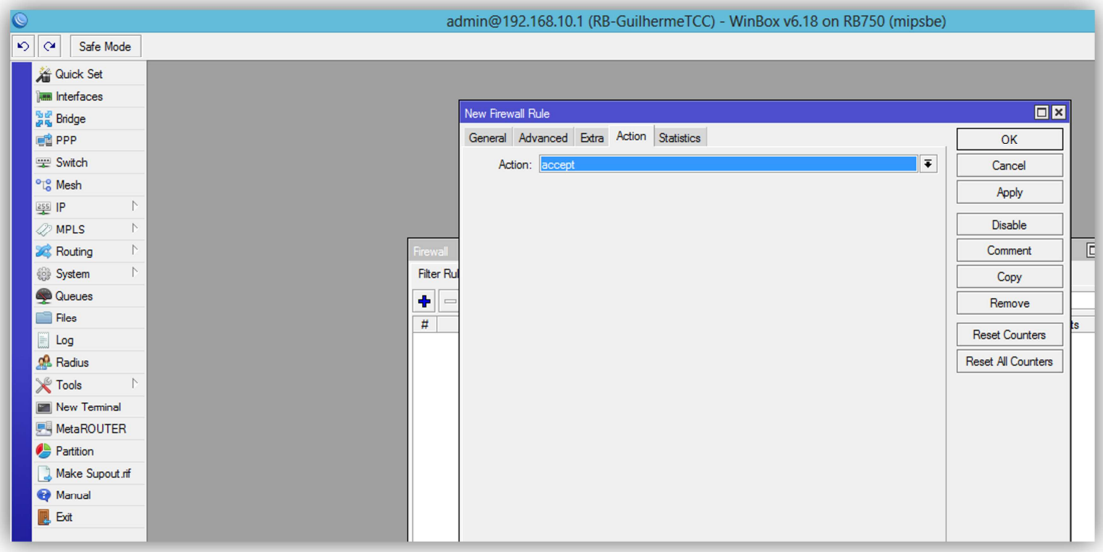


Imagem 34: Tela de criação de regras do Firewall

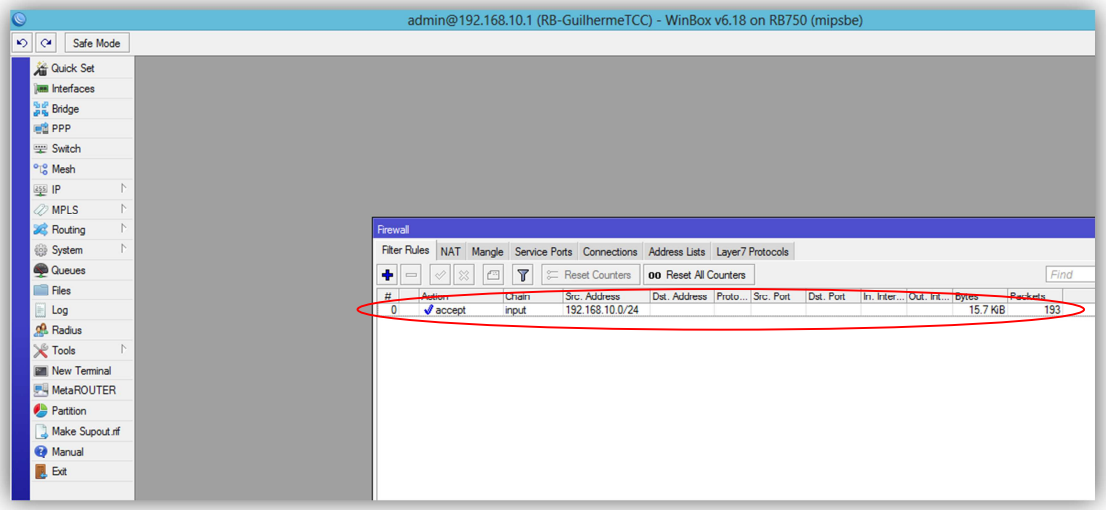


Imagem 35: Após a inclusão de uma regra no Firewall

Essa regra fará com que todo o tráfego que entre na Routerboard**(input)** e que tenha origem da classe 192.168.10.0/24**(Src.Address)** seja aceito e liberado**(accept)**.

9.2. ADICIONANDO REGRAS DE NAT

9.2.1 ADICIONANDO REGRAS DE MASCARAMENTO DE IP

Agora iniciaremos a inclusão de uma regra de NAT em nossa Routerboard. Entraremos no Menu: **IP=>Firewall** e clicaremos na guia NAT, em seguida na opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida uma tela de **New NAT Rule** como mostra a imagem abaixo.

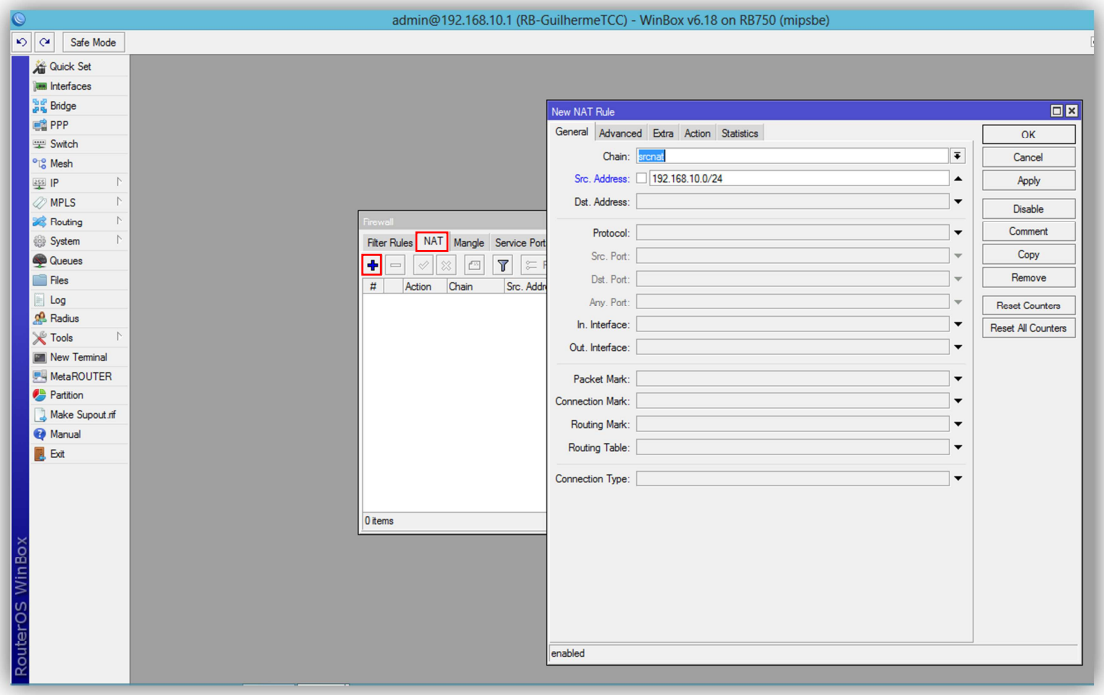


Imagem 36: Tela de inclusão de uma regra de NAT

No campo **Chain** selecionaremos a opção srcnat, e no campo **Src.Address** colocaremos a classe e a máscara de sub-rede de nossa rede 192.168.10.0/24, ou seja, são os pacotes que vierem da rede 192.168.10.0/24 sairão para a Internet com o endereço de ip público disponibilizado pela interface UpLink, devemos clicar na guia Action e no campo **Action** selecionar a opção masquerade e em seguida OK.

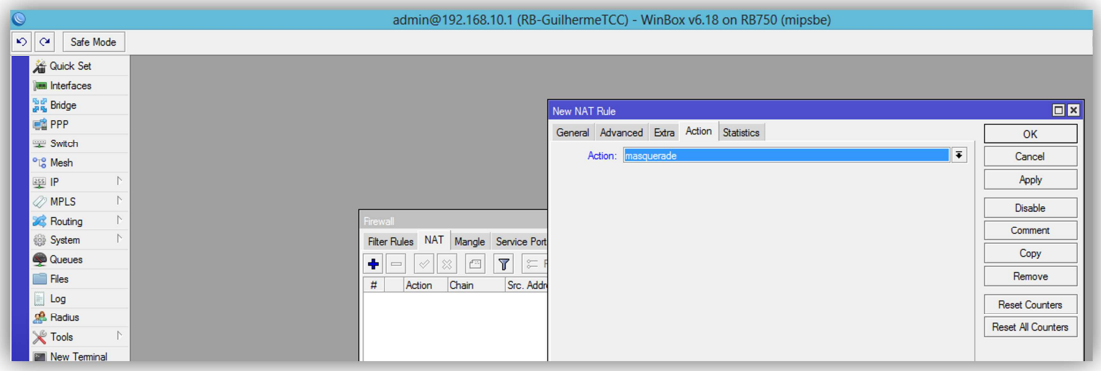


Imagem 37: Tela de inclusão de uma regra de NAT

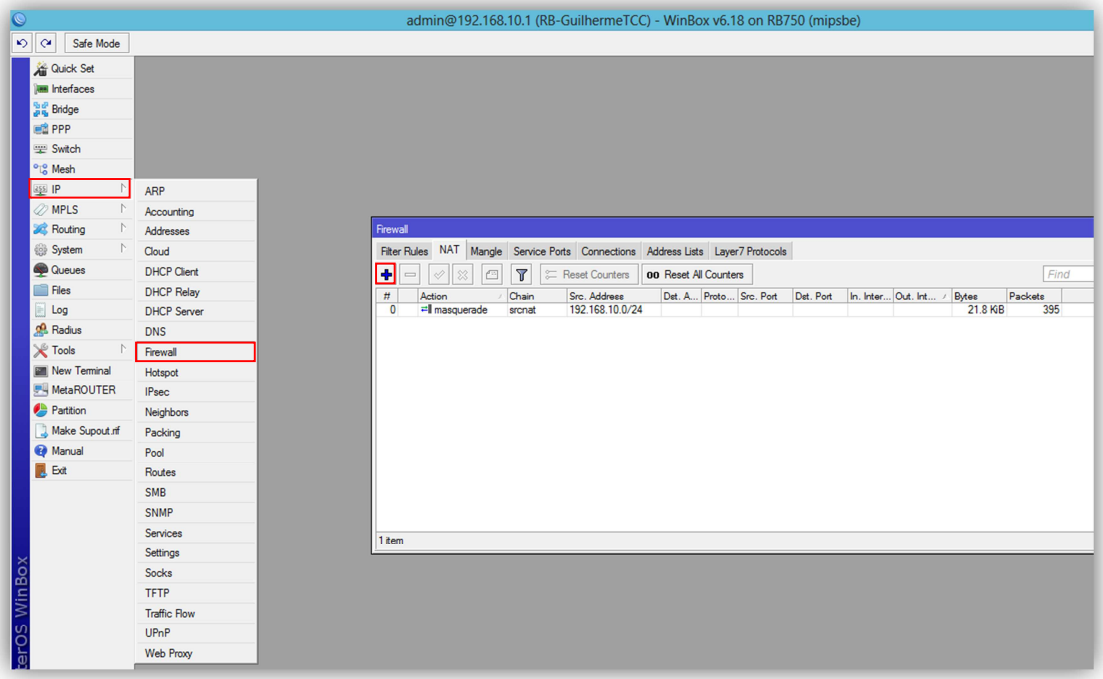


Imagem 38: Após a inclusão de uma regra de NAT

Essa regra fará que todo o tráfego de pacotes que vierem**(srcnat)** da classe 192.168.10.0/24**(Src.Address)** sejam traduzidos**(masquerade)** do endereço de rede local para o endereço de ip público disponibilizado pela interface UpLink ao sair para a internet.

9.2.2 ADICIONANDO REGRAS DE REDIRECIONAMENTO DE PORTA

Agora vamos criar uma regra de NAT para o redirecionamento da porta 80(http) para a porta do nosso Web Proxy, que será configurado nos tópicos a seguir, usaremos a porta 3128 para o webproxy.

No campo **Chain** selecionaremos a opção dstnat, no campo **Src.Address** colocaremos a classe e a máscara de sub-rede de nossa rede 192.168.10.0/24, no campo **Protocol** selecionaremos a opção 6(tcp) e **Dst.Port**. colocaremos a porta 80, após isso devemos clicar na guia Action e no campo **Action** vamos selecionar a opção redirect e na opção **To Ports** colocaremos a porta 3128, em seguida clicaremos em OK.

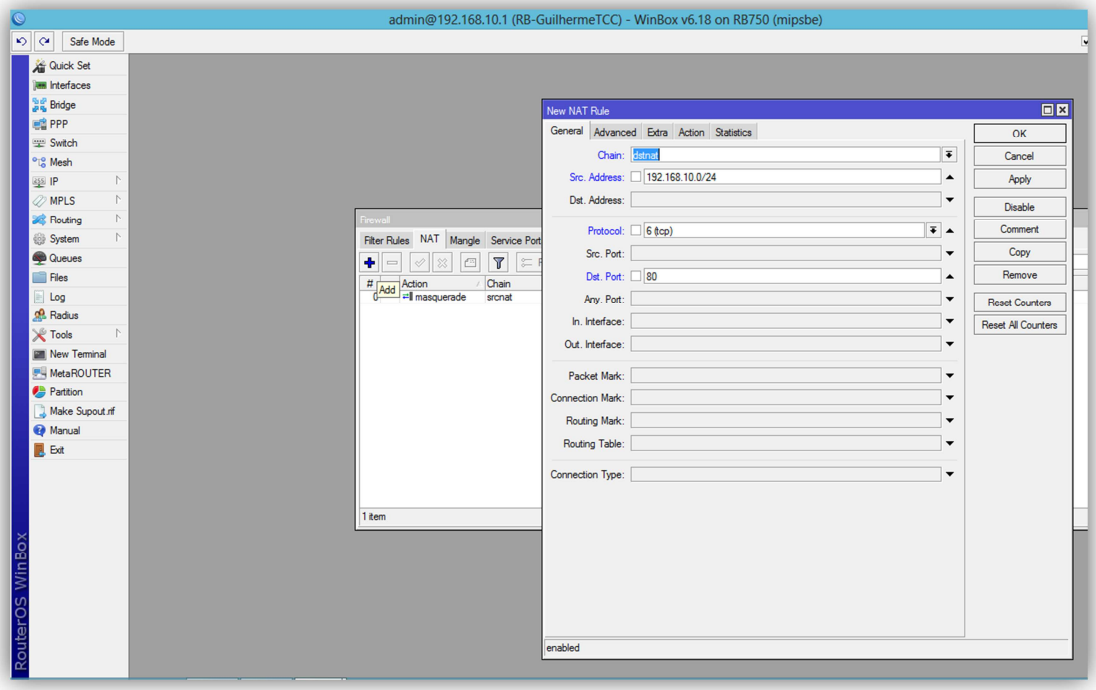


Imagem 39: Tela de inclusão de uma regra de NAT

Essa regra fará que todo o tráfego de pacotes que trafegarem com destino**(dstnat)** à classe 192.168.10.0/24**(Src.Address)** sejam redirecionados**(redirect)** da porta 80(**Dst.Port**) para a porta 3128(**To Ports**) antes que sejam liberados para o usuário.

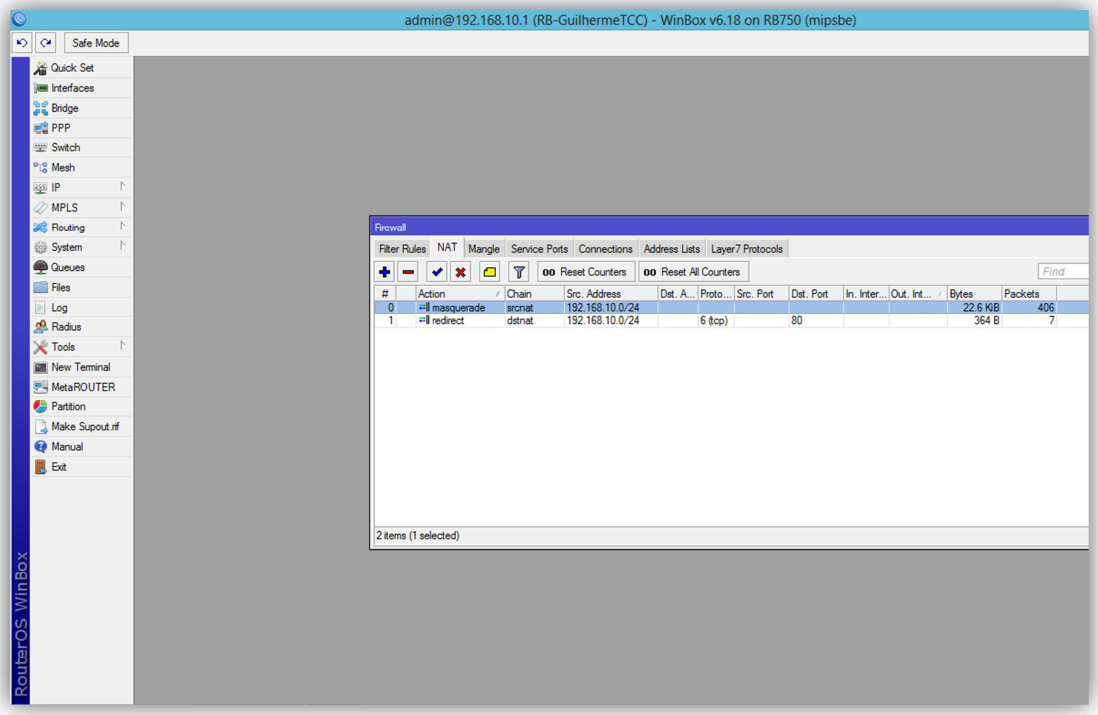


Imagem 40: Tela após a inclusão das regras de NAT

10. WEBPROXY

10.1. CONFIGURANDO O WEB PROXY

Agora iniciaremos a configuração de nosso Web Proxy. Entraremos no Menu: **IP=>Web Proxy** e clicaremos na opção Enable, habilitando assim o nosso Web Proxy. Colocaremos a porta 3128 como a porta do Web Proxy, que será a porta que o NAT fará o redirecionamento da porta 80 para a 3128, como configuramos anteriormente no **Firewall=>NAT.**

No campo **Cache Administrator** colocaremos um nome ou email de referência para que o usuário que sofre algum bloqueio e necessite de suporte consiga contactar o responsável pelas regras do Web Proxy, nesse caso colocaremos o email guilhermelevy.cpd@faculdadeguairaca.com.br

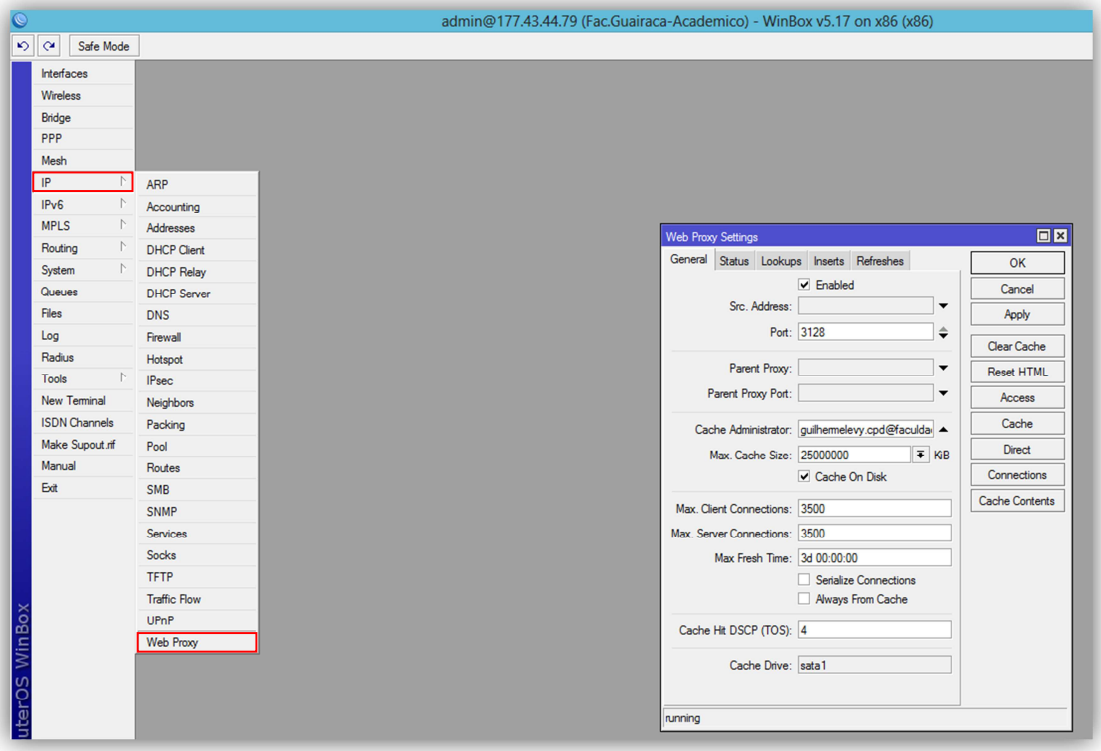


Imagem 41: Tela de configuração inicial do Web Proxy

A opção **Max.Cache Size** serve para quando o administrador deseja criar uma área no armazenamento do RouterOS para fazer um cache no Web Proxy, ele colocará uma quantidade, por exemplo 500000KiB (500MB) e marcará a opção **Cache On Disk**. No nosso caso, por utilizarmos uma Routerboard com pouco espaço de armazenamento não utilizaremos essa opção de Cache On Disk.

Na opção **Max.Client Connections**, que seria a quantidade máxima de conexões simultâneas no proxy deixaremos 1500. Na opção **Max.Server Connections**, que seria a quantidade máxima de conexões simultâneas no proxy para servidores externos deixaremos 1500.

Os demais campo deverão ficar no padrão do RouterOS como a Imagem41.

10.2. ADICIONANDO REGRAS NO WEB PROXY

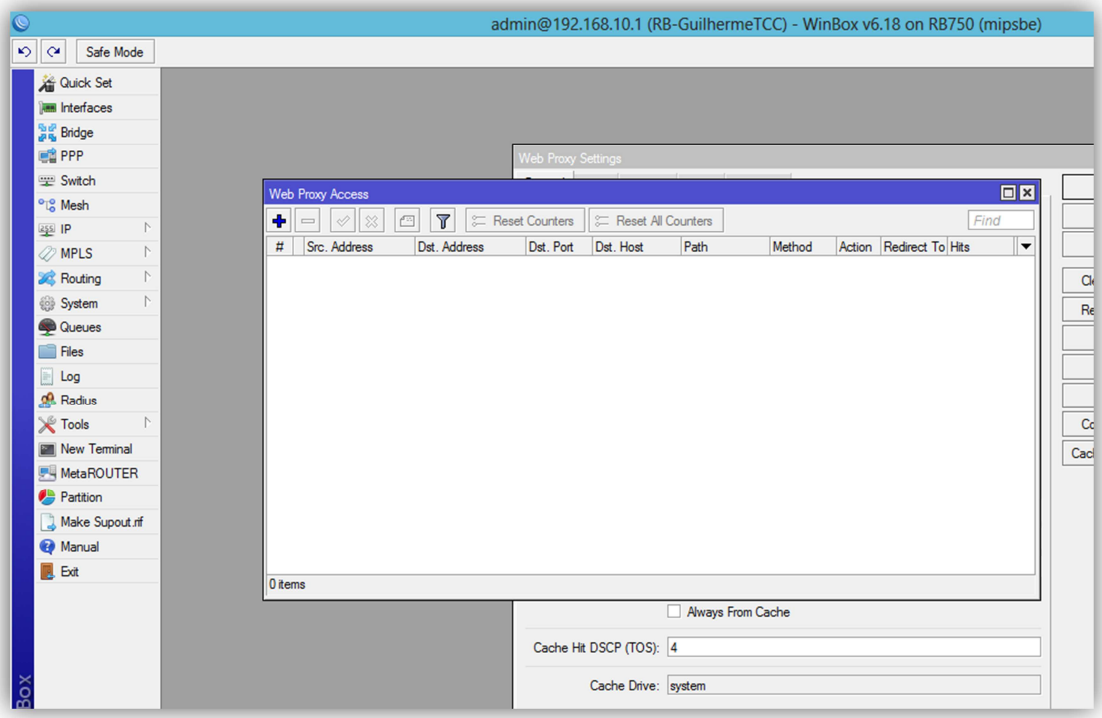


Imagem 42: Tela de configuração das regras do Web Proxy

Após a configuração inicial do Web Proxy podemos iniciar a criação das regras, clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚ .

Primeiramente criaremos a liberação da classe da nossa rede, no campo **Src.Address** colocaremos a classe da rede que queremos que essa regra se aplique, nesse caso 192.168.10.0/24 e no campo **Action** selecionaremos a opção allow que libera o trafego para essa rede.

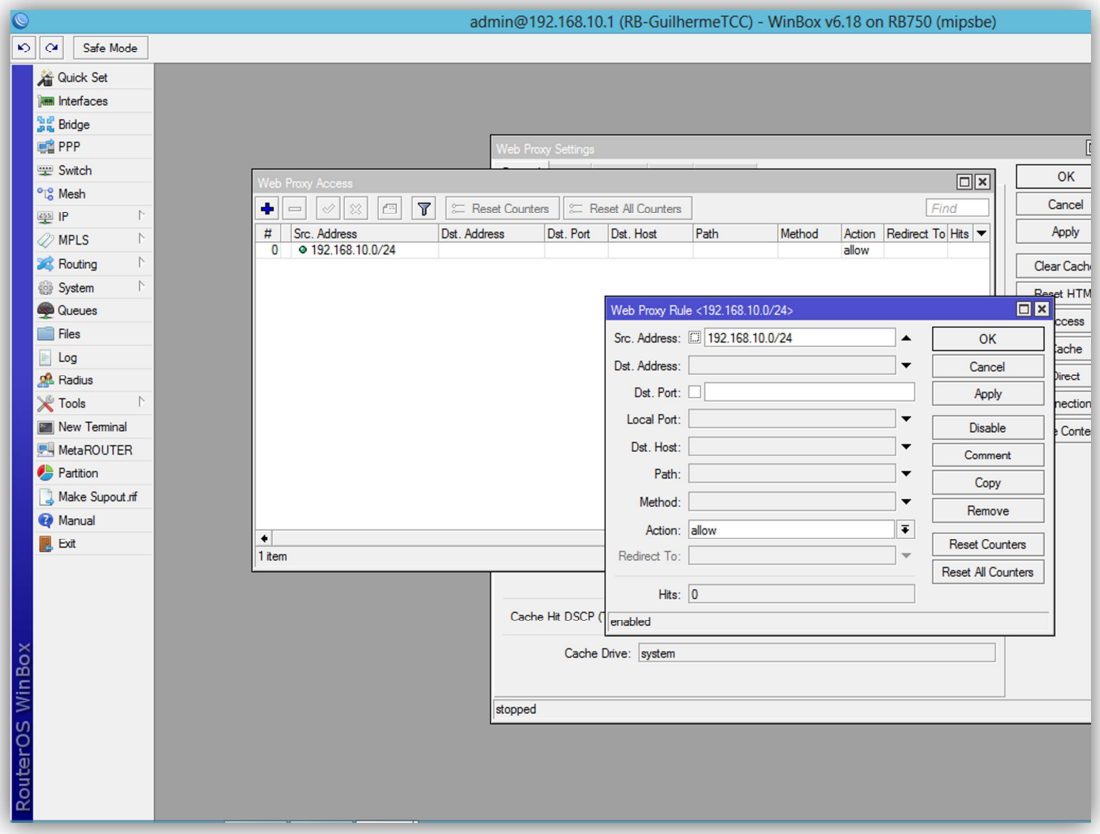


Imagem 43: Liberando o tráfego da classe principal

10.3. BLOQUEANDO TERMOS NO WEBPROXY

Agora criaremos duas regras de bloqueio para dois termos(palavras) dentro de nosso Web Proxy, no caso de regras de bloqueio por palavras preencheremos somente o campo **Dst.Host** com a palavra a ser bloqueada e no campo **Action** selecionaremos a opção deny que nega o tráfego dos dados que contenham essa palavra em seus endereços, ou seja, o Web Proxy bloqueará as páginas HTTP que contenham em seu endereço a palavra especificada.

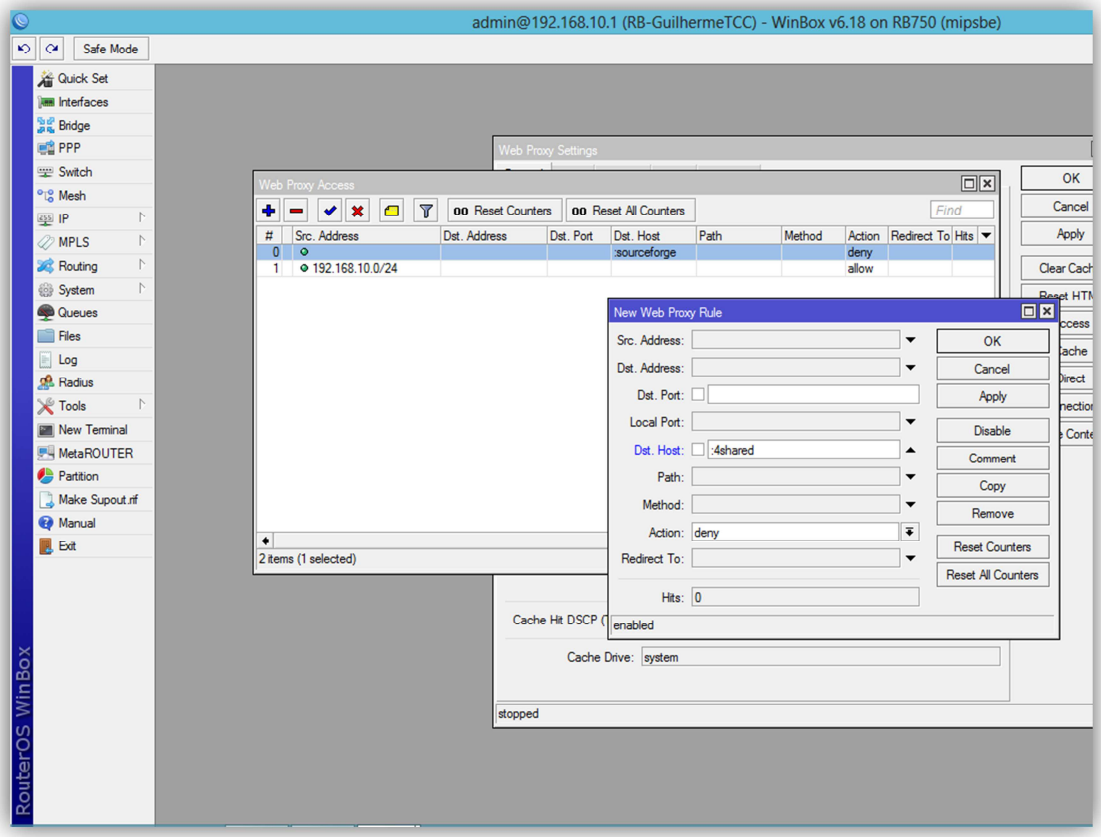


Imagem 44: Bloqueando o termo “4shared”

Nessas duas regras nós bloqueamos as palavras “4shared” e “sourceforge”.

10.4. O FUNCIONAMENTO DO WEB PROXY

Como em todas a regras do RouterOs, o Web Proxy trata suas regras através do princípio da gravidade, o sistema começa a leitura das regras por ordem, seguindo sua numeração(#), ou seja, de cima para baixo e para ao se adequar em uma das regras.

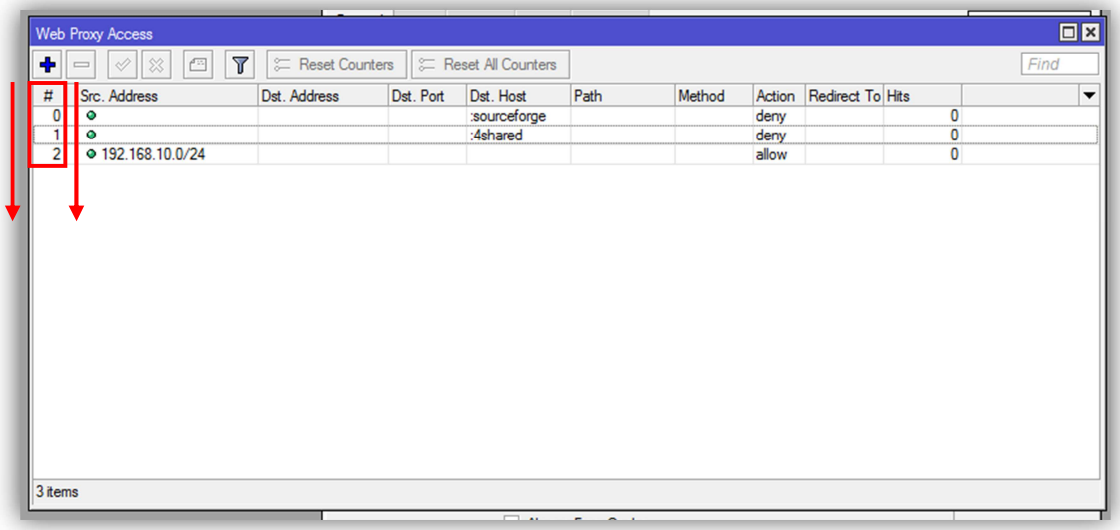


Imagem 45: Adequação da regra por gravidade

Como nos mostra a Imagem45, se o usuário com o endereço de ip 192.168.10.5 tentar acessar o site www.uol.com.br o pacote irá testar todas as regras e como não há nenhuma restrição nos itens 0 e 1 chegará ao item 3, se adequando a essa regra que libera o tráfego para a classe na qual ele se encontra. Se esse mesmo usuário tentar acessar o site www.4shared.com ele testaria a regra 0, passaria para a próxima regra mas se adequaria à regra 1 em que ele bloqueia os endereços com a palavra 4shared, descartando nessa hora o pacote sem passar para a próxima regra.

Nas duas imagens abaixo podemos visualizar como será a mensagem de negação no microcomputador do usuário quando ele tentar acessar um dos sites que estiverem com as regras de bloqueio.

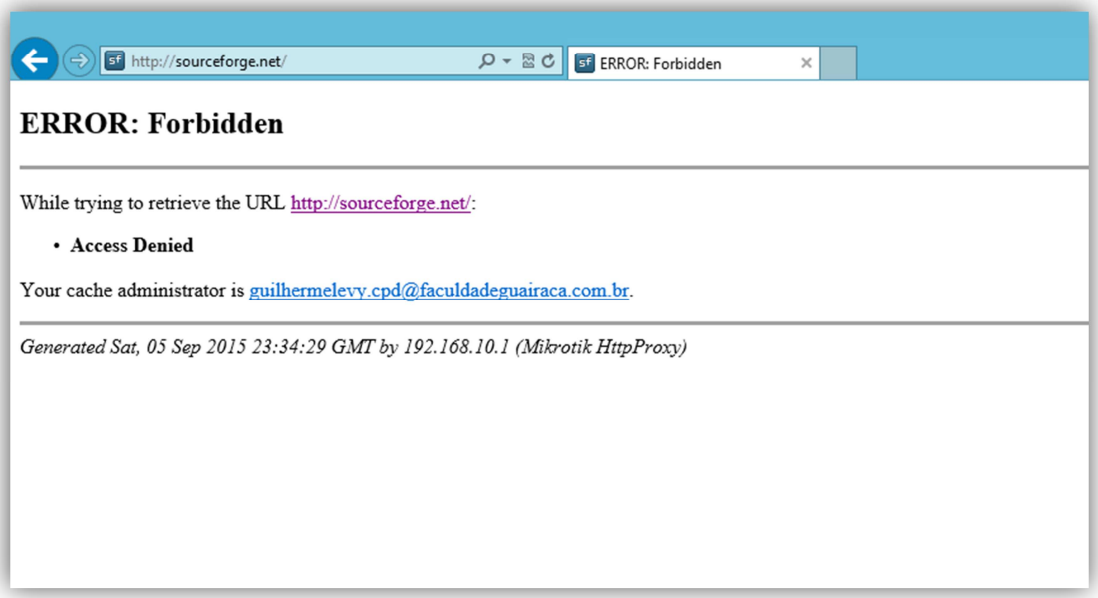


Imagem 46: Tela com a negação do site sourceforge.net

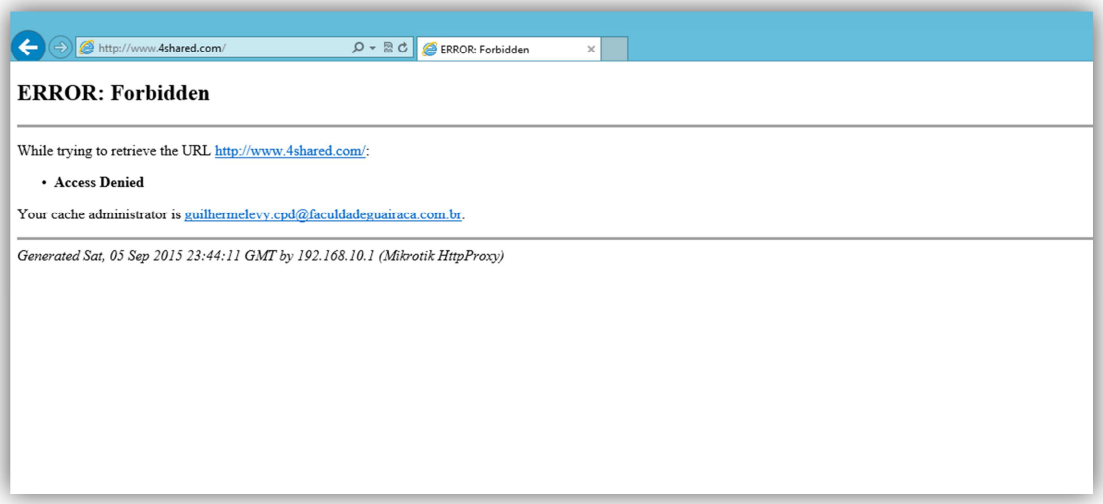


Imagem 47: Tela com a negação do site 4shared.com

11. HOTSPOT

Com a estrutura de nossa rede finalizada podemos agora iniciar a criação e configuração de nosso servidor Hotspot. Entraremos no Menu: **IP=>Hotspot,** na guia **Servers** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

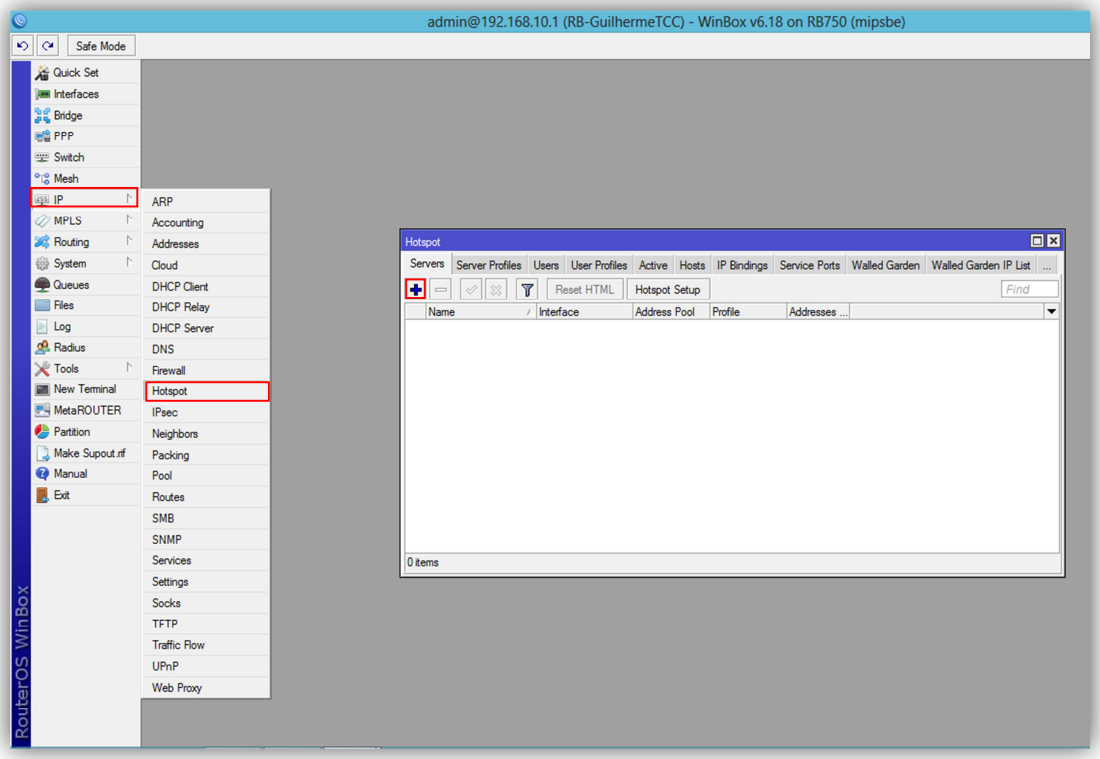


Imagem 48: Tela inicial de configuração de um Hotspot Server

11.1. ADICIONANDO UM HOTSPOT SERVER

No campo **Name** colocaremos o server1, que será o nome do nosso servidor Hotspot, no campo **Interface** selecionaremos a interface que será responsável por fornecer os dados já tratados pelo nosso hotspot, no campo **Address Pool** escolheremos qual a faixa de endereços que queremos que o hotspot forneça aos usuários que nele se conectarem, o campo **Idle TimeOut** será o período de ociosidade máximo permitido por nosso servidor para os clientes autenticados, se não houver trasmissão de dados para o servidor nesse período a sessão com esse usuário será finalizada, deixaremos 02:00:00 horas nesse campo e para finalizar o campo **Addresses per MAC** que é a quantidade de endereços de ip permitidos para cada endereço MAC dos clientes, deixaremos 2, pois se o cliente vier com seu microcomputador ou dispositivo já com um ip configurado manualmente e que não seja da classe de nossa rede o hotspot automaticamente lhe fornecerá um endereço de ip da nossa rede para que ele possa trafegar nela, vinculando assim os dois endereços de ip a esse endereço MAC. Os demais campos permanecem no padrão do RouterOS.

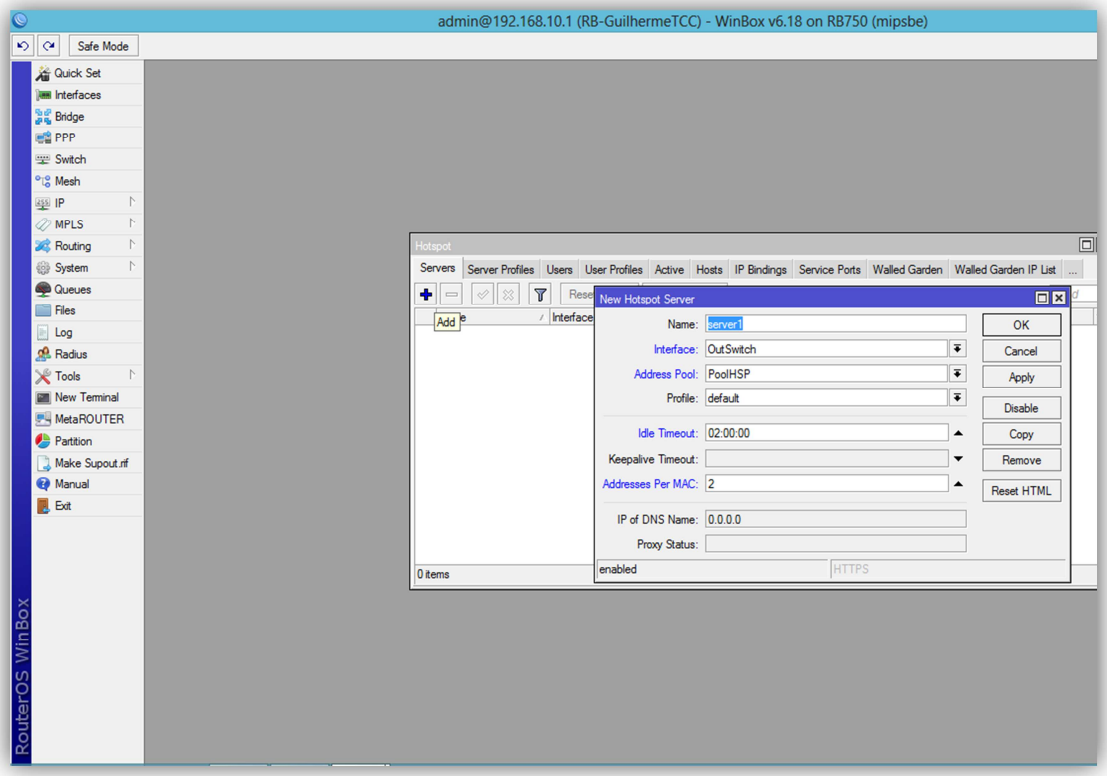


Imagem 49: Tela de inclusão de um Hotspot Server

Na imagem abaixo podemos visualizar como ficará a tela inicial do hotspot após a inclusão de um servidor hotspot.

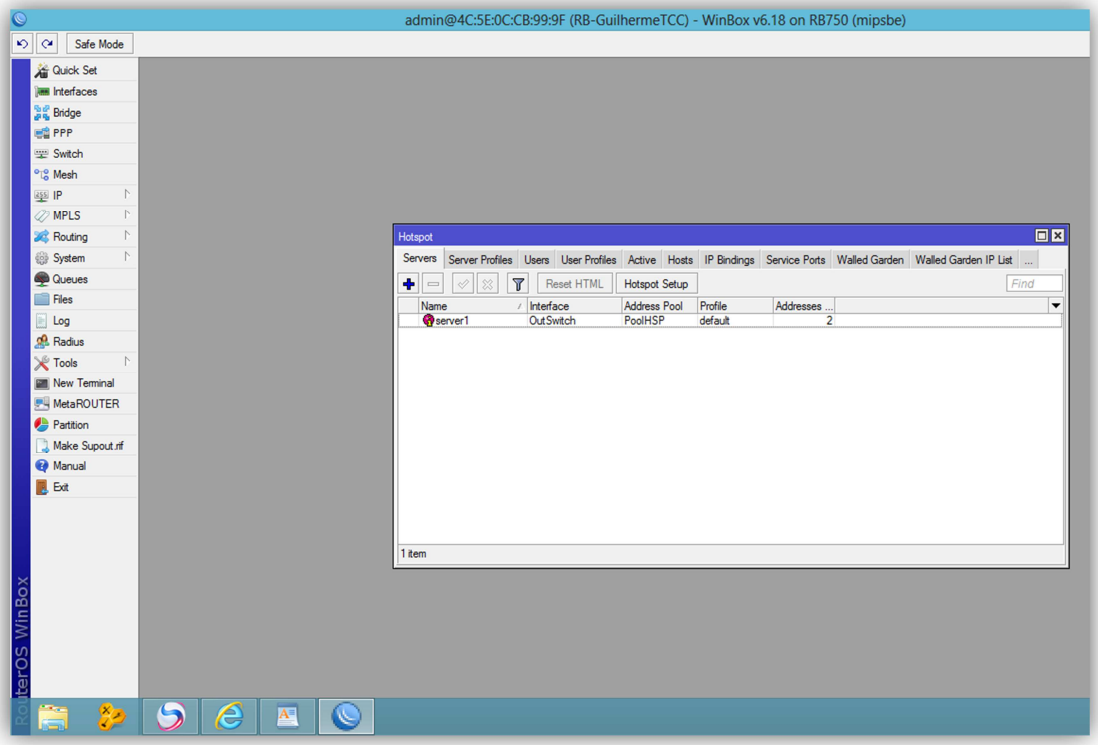


Imagem 50: Tela após a inclusão de um Hotspot Server

11.2. CONFIGURANDO UM HOTSPOT SERVER PROFILE

Agora iremos configurar o perfil default do servidor hotspot. Entraremos no Menu: **IP=>Hotspot** e clicaremos na guia Server Profiles, em seguida daremos um duplo clique encima do perfil padrão existente em nosso hotspot, o perfil default.

Nesse perfil existente somente iremos alterar o campo **DNS Name**, que é o nome pelo qual nosso hotspot será identificado e acessado manualmente, colocaremos hotspottcc.com.br nesse campo. O DNS Name aparecerá na tela de login do hotspot e irá mascarar o endereço de ip do hotspot. Agora clicaremos em OK finalizando a configuração.

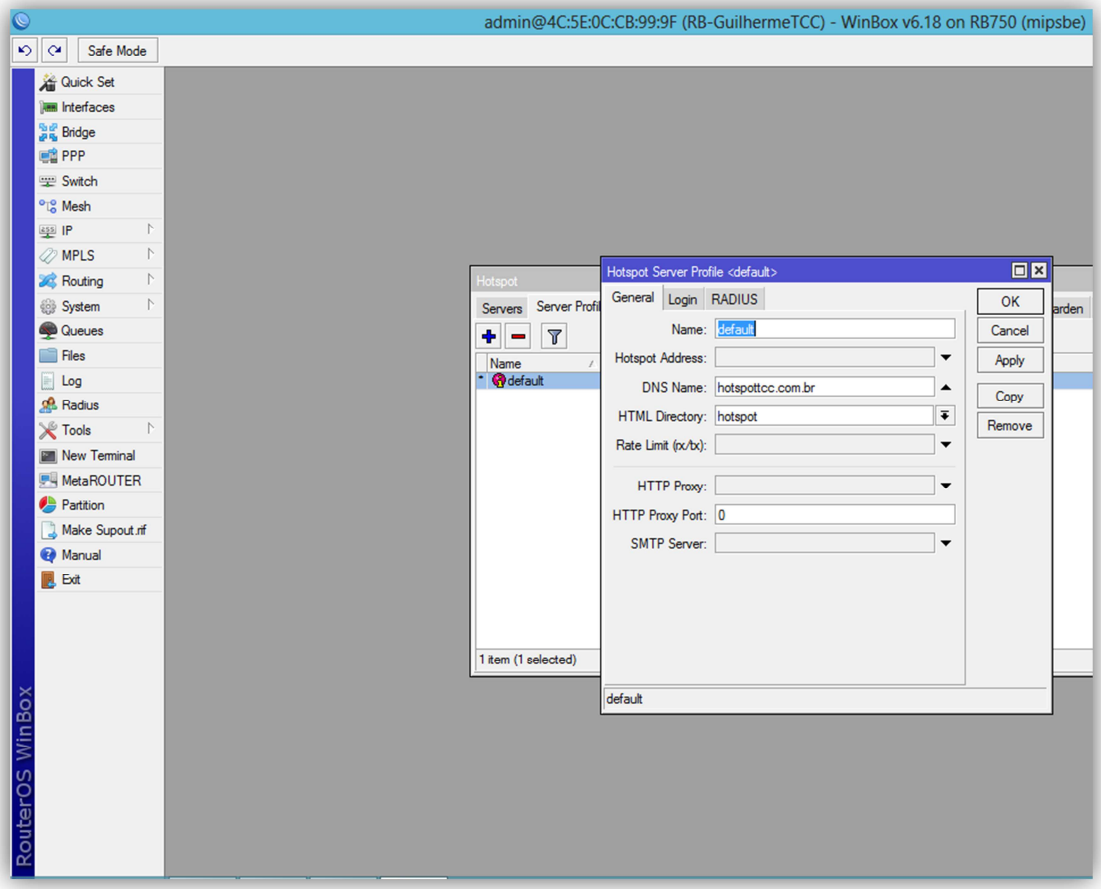


Imagem 51: Configuração do Hotspot Server Profile default

Os demais campos devem permanecer no padrão do RouterOS, conforme a Imagem51.

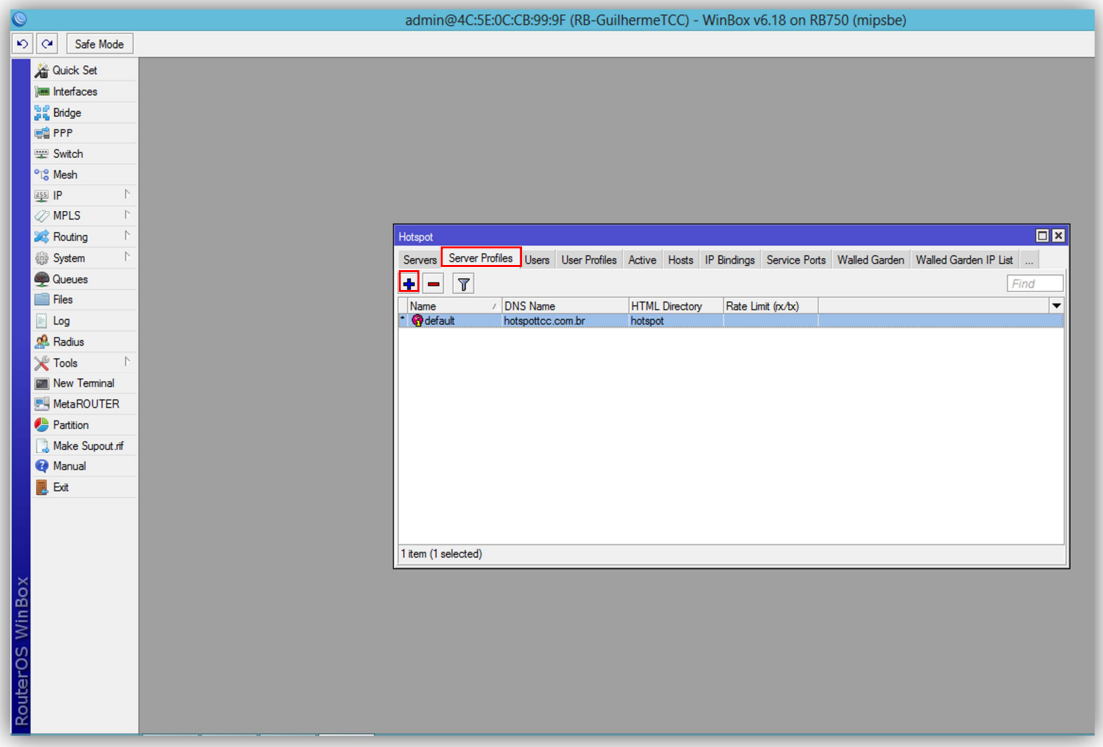


Imagem 52: Tela após a inclusão de um Hotspot Server Profile

11.3. CONFIGURANDO UM HOTSPOT USER PROFILE

Primeiramente iremos configurar o perfil default de usuário do hotspot. Entraremos no Menu: **IP=>Hotspot** e clicaremos na guia User Profiles, em seguida daremos um duplo clique encima do perfil padrão existente em nosso hotspot, o perfil default.

Deixaremos o **Name** como default, no campo **Address Pool** selecionaremos o Pool de endereços de ip que fornecerá o ip ao nosso cliente após a autenticação, no campo **Idle Timeout** selecionaremos a opção none, ou seja, não finalizará a sessão se o usuário ficar um período de tempo ocioso. O campo **Shared Users** nos diz quantos usuários simultâneos com a mesma credencial poderão estar autenticados, em nosso caso permitiremos um usuário autenticado com a mesma credencial. O campo **Rate Limit** é responsável pelo limite de banda de perfil de usuário, iremos colocar 5Mb de upload e 5Mb de download para cada um dos usuários autenticados com esse perfil, ou seja, 5M/5M. Os demais campos deverão ficar no padrão do RouterOS, como na imagem abaixo.

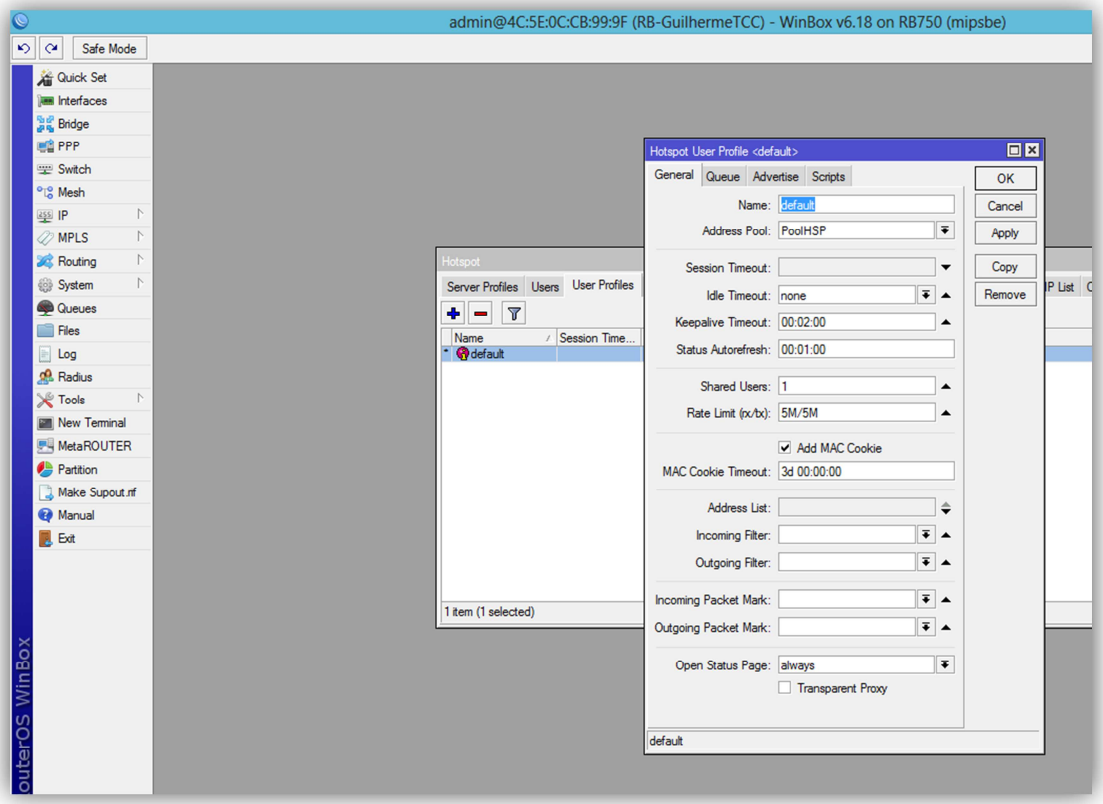


Imagem 53: Tela após a inclusão de um Hotspot User Profile

Seguindo os passos anteriores para a configuração de um User Profile, faremos também a inclusão de um User Profile Limitado em nosso hotspot. Clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida uma tela de **New User Profile**.

Daremos o nome de limitado a esse perfil e no campo **Rate Limit** daremos um limite de banda de 1Mb de upload e 1Mb de download para cada um dos usuários autenticados nesse perfil, ou seja, 1M/1M

Após a inclusão dos dois perfis de usuário a tela de User Profiles deverá estar como a imagem abaixo.

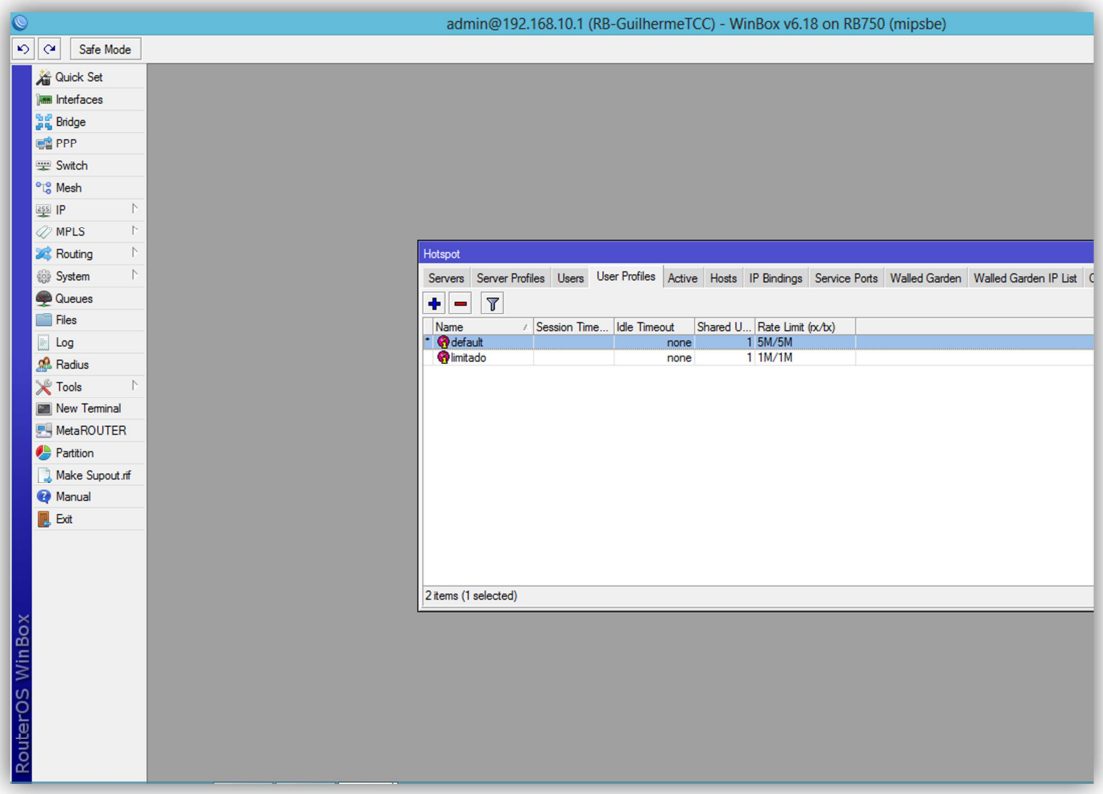


Imagem 54: Tela após a inclusão dos Hotspot User Profile

11.4. ADICIONANDO USUÁRIOS

Agora iremos criar os usuários que poderão autenticar em nosso hotspot, clicaremos na guia User e na tela inicial de usuários clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida a tela **Hotspot User**, que é a tela de inclusão de usuários, como na Imagem56.

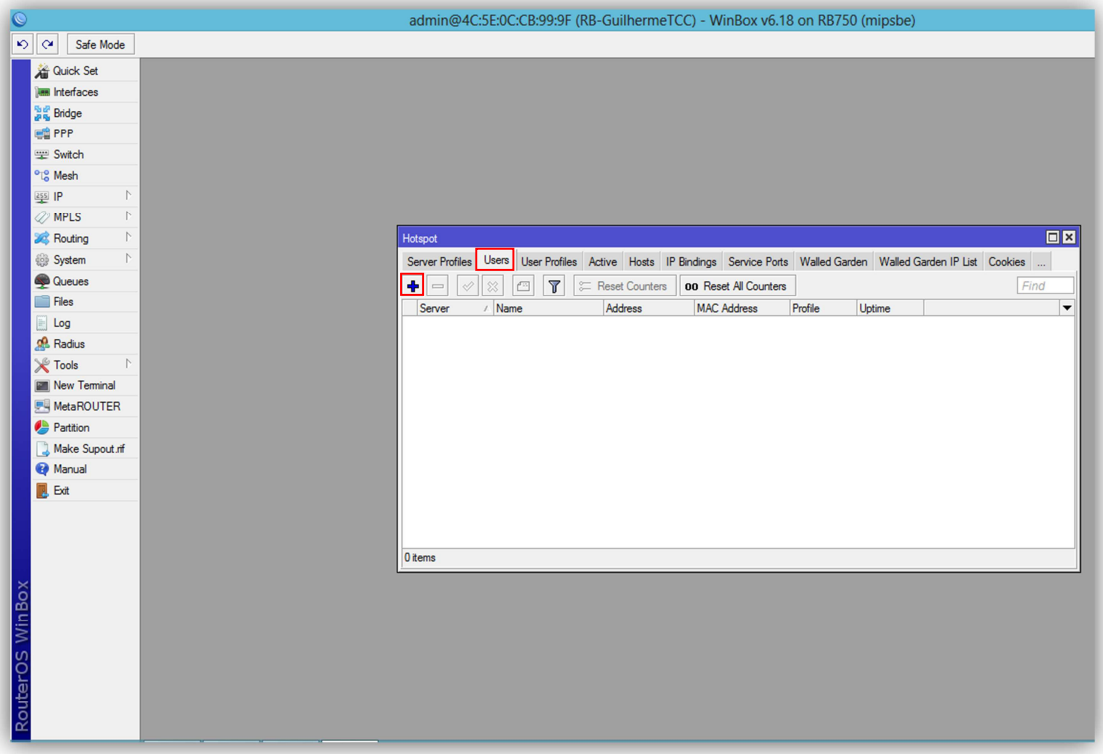


Imagem 55: Tela inicial dos usuários cadastrados no Hotspot

11.4.1. USUÁRIO AUTENTICANDO COM SENHA

No campo **Name** colocaremos o nome que nosso usuário efetuará a autenticação, no campo **Password** colocaremos a senha que o usuário utilizará, no nosso caso utilizaremos o usuário e senha admin.

O campo **Address** não será alterado, esse campo é utilizado quando desejamos dar um ip estático para um determinado usuário. No campo **Profile** selecionaremos o perfil que esse usuário estará vinculado quando se autenticar, nesse caso ele será vinculado ao perfil default, que possui um limite de banda maior, conforme especificamos no Hotspot Users Profile anteriormente. Os demais campos devem ficar no padrão do RouterOS, como mostra a imagem abaixo.

Esse modo de autenticação estará disponível ao cliente que possuir usuário e senha cadastrado, podendo ser utilizado esse usuario e senha em qualquer microcomputador ou dispositivo.

Criaremos também um segundo usuário com o nome de user e nele utilizaremos o perfil limitado, que disponibiliza menos limite de banda, conforme o User Profile.

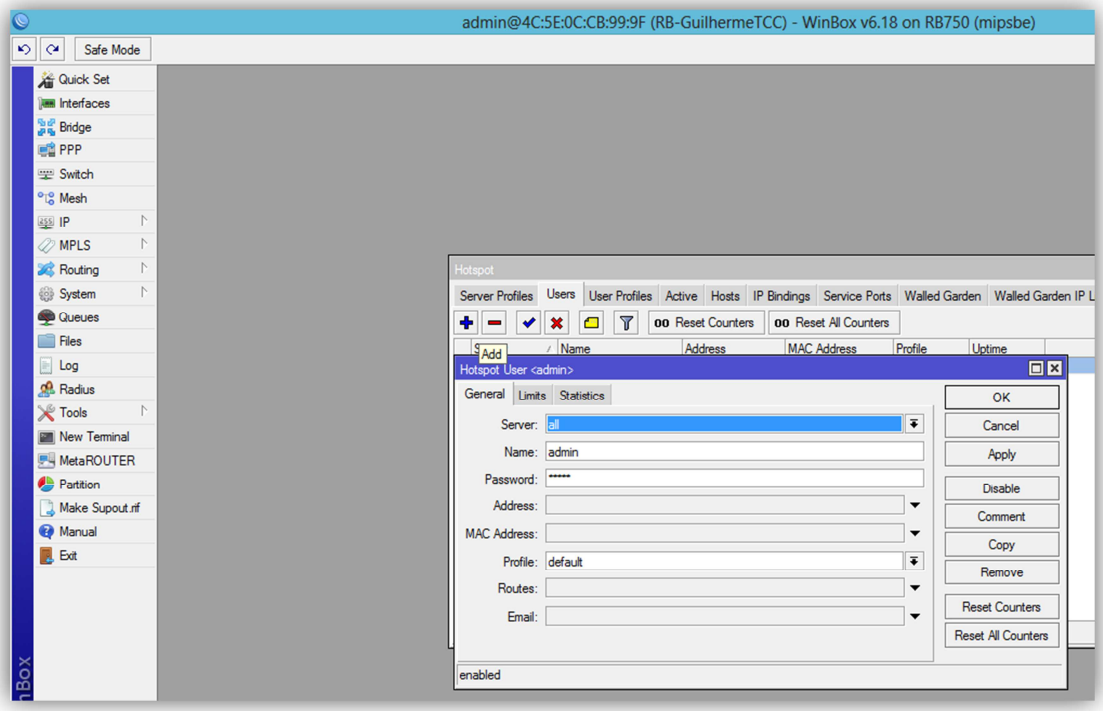


Imagem 56: Tela de inclusão de usuário/senha

11.4.2. USUÁRIO AUTENTICANDO COM MAC

No campo **Name** colocaremos o nome que nosso usuário efetuará a autenticação, no nosso caso utilizamos o usuário usermac. No campo **MAC** colocaremos o endereço MAC do microcomputador ou dispositivo do nosso cliente e no campo **Profile** selecionaremos o perfil Limitado.

Os demais campos devem ficar no padrão do RouterOS, como mostra a imagem abaixo.

Esse modo de autenticação não necessitará que o cliente possua uma senha para seu usuário, pois fará uma verificação do vínculo entre o nome de usuário e o endereço MAC do micromputador ou dispositivo em que se está sendo feito a autenticação, se for o endereço MAC correto o hotspot irá autenticá-lo, neste tipo de autenticação usuário/MAC o cliente somente poderá utilizar suas credencias no micromputador ou dispositvo que tiver o MAC cadastrado em seu usuário.

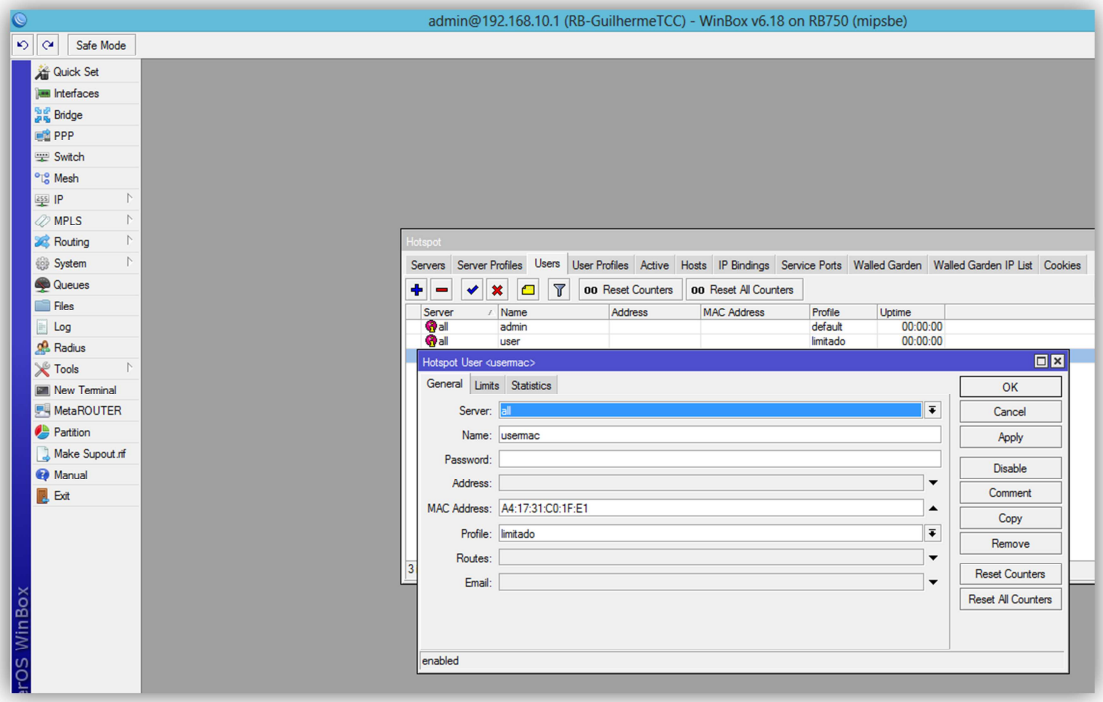


Imagem 57: Tela de inclusão de usuário/MAC

Na imagem abaixo podemos visualizar como ficará a tela inicial da lista de usuários cadastrados em nosso hotspot após a inclusão dos usuários.

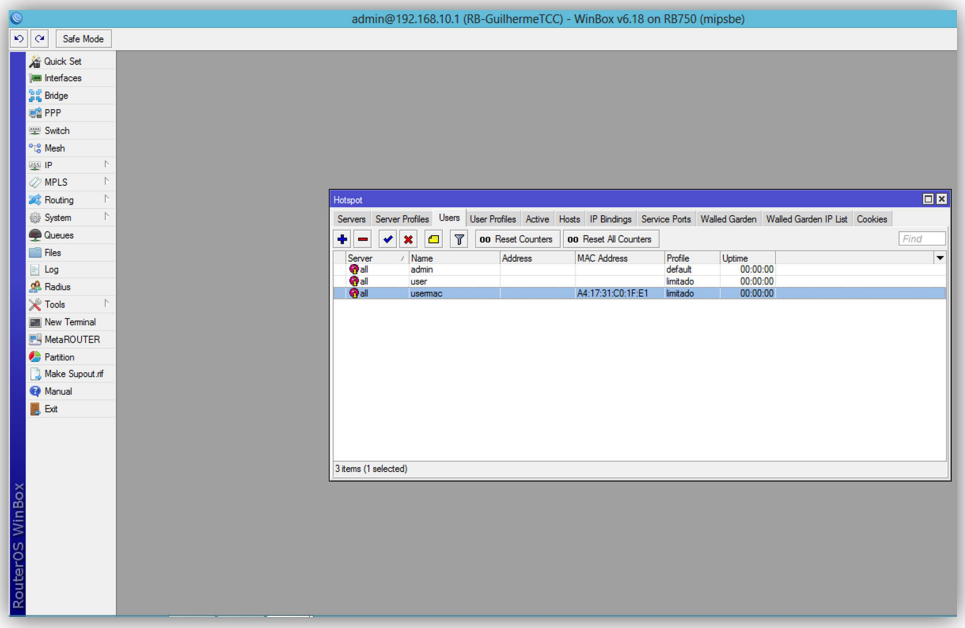


Imagem 58: Tela após a inclusão dos usuários

11.5. CONFIGURAÇÕES DO HOTSPOT NO FIREWALL E NAT

Ao ser criado o Hotspot cria automaticamente regras no Firewall, essas regras acabam bloqueando o acesso do Winbox à Routerboard, então após a criação do Hotspot devemos nos conectar ao RouterOS pelo endereço MAC da Routerboard como na Imagem abaixo, assim como fizemos no inicio deste manual na Imagem03.

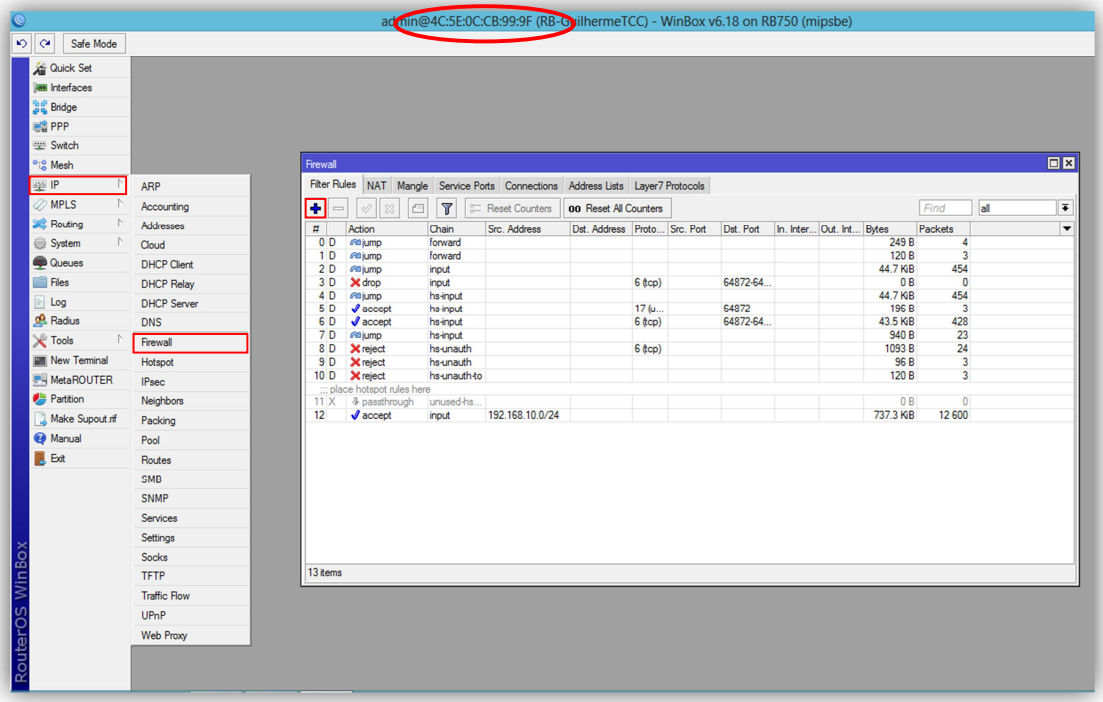


Imagem 59: Liberando acesso do Winbox no Firewall

Agora iniciaremos a inclusão da regra de liberação no **Firewall** em nosso RouterOS. Entraremos no Menu: **IP=>Firewall** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida uma tela de **Firewall Rule** como a Imagem60.

No campo **Chain** selecionaremos a opção forward, ou seja, é todo o tráfego que passa pela Routerboard, no campo **Protocol** selecionaremos a opção 6(tcp) e no campo **Dst.Port** colocaremos a porta 8291, que é a porta por onde o Winbox se comunica com o RouterOS, após isso devemos clicar na guia Action e no campo **Action** selecionar a opção accept e em seguida OK.

Os demais campo deverão permanecer no padrão do RouterOS, como na imagem abaixo.

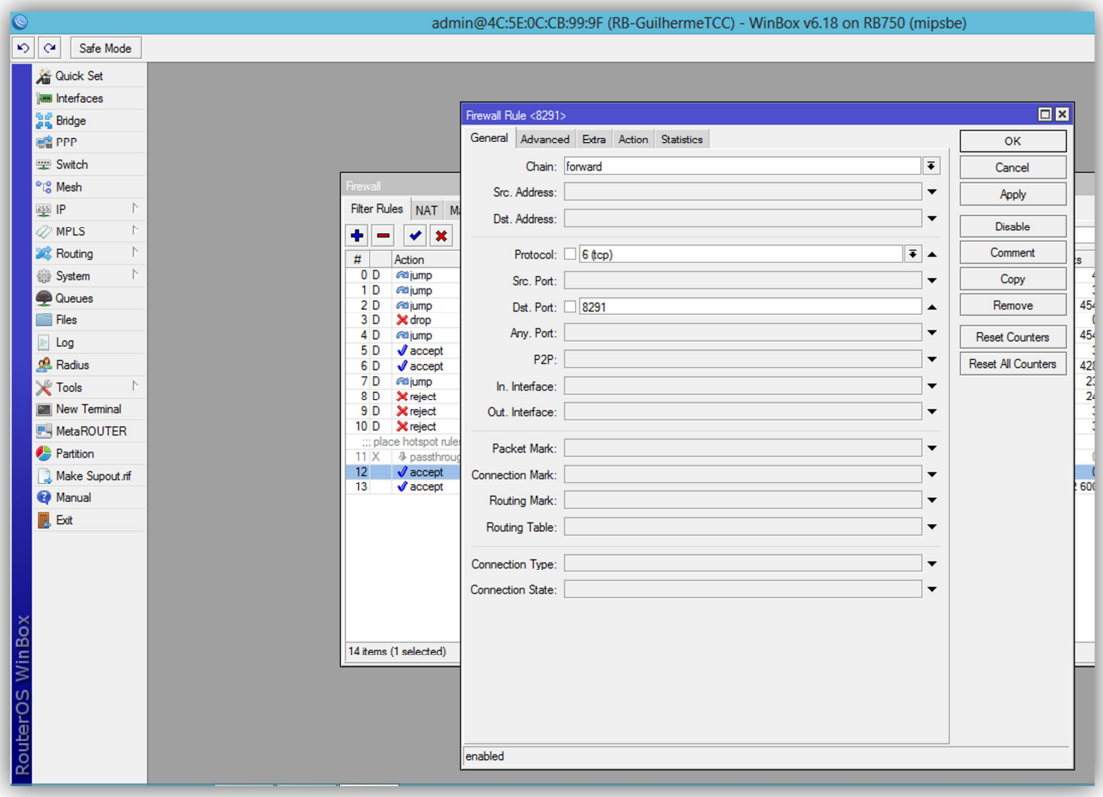


Imagem 60: Criando regra de acesso do Winbox

Na imagem abaixo podemos visualizar como ficará a tela inicial do Firewall após a inclusão da regra de liberação do acesso do Winbox ao RouterOS.

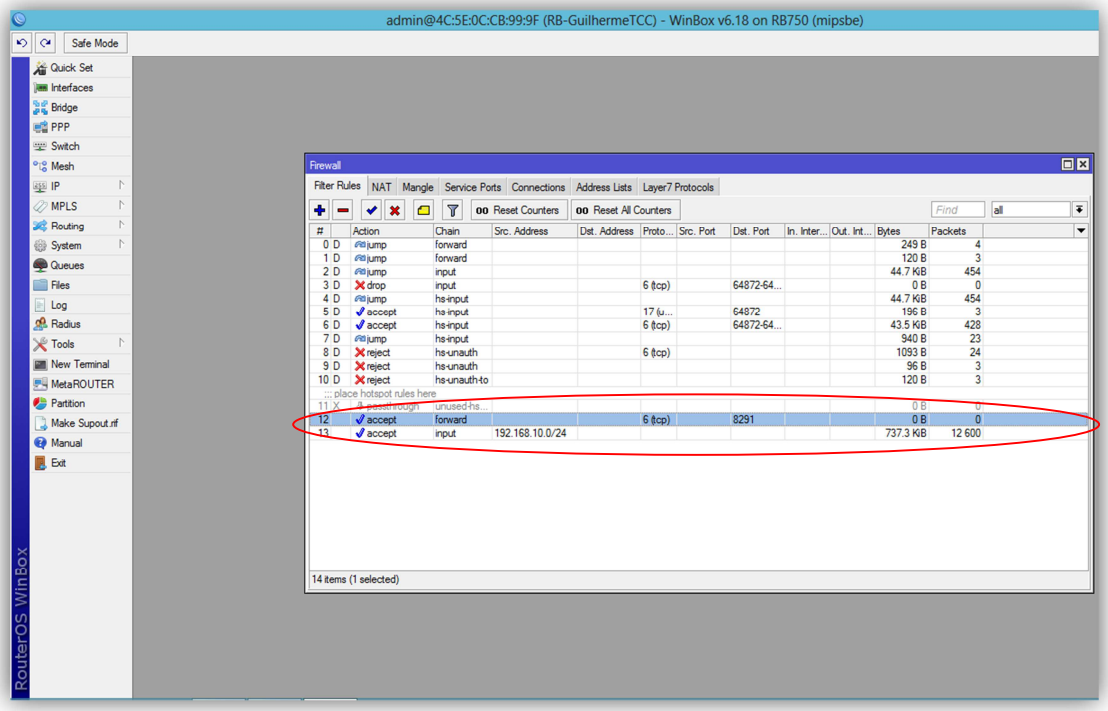


Imagem 61: Firewall após a inclusão da regra de acesso do Winbox

Após a criação dessa regra podemos novamente nos conectar ao RouterOS pelo endereço de ip como efetuado anteriormente e pode ser visualizado na Imagem23 deste manual, pois essa regra irá liberar o acesso do Winbox ao RouterOS.

O Hotspot também cria automaticamente regras no NAT ao ser configurado, nesse caso não é necessário fazer nenhuma configuração nas regras criadas dinamicamente por ele.

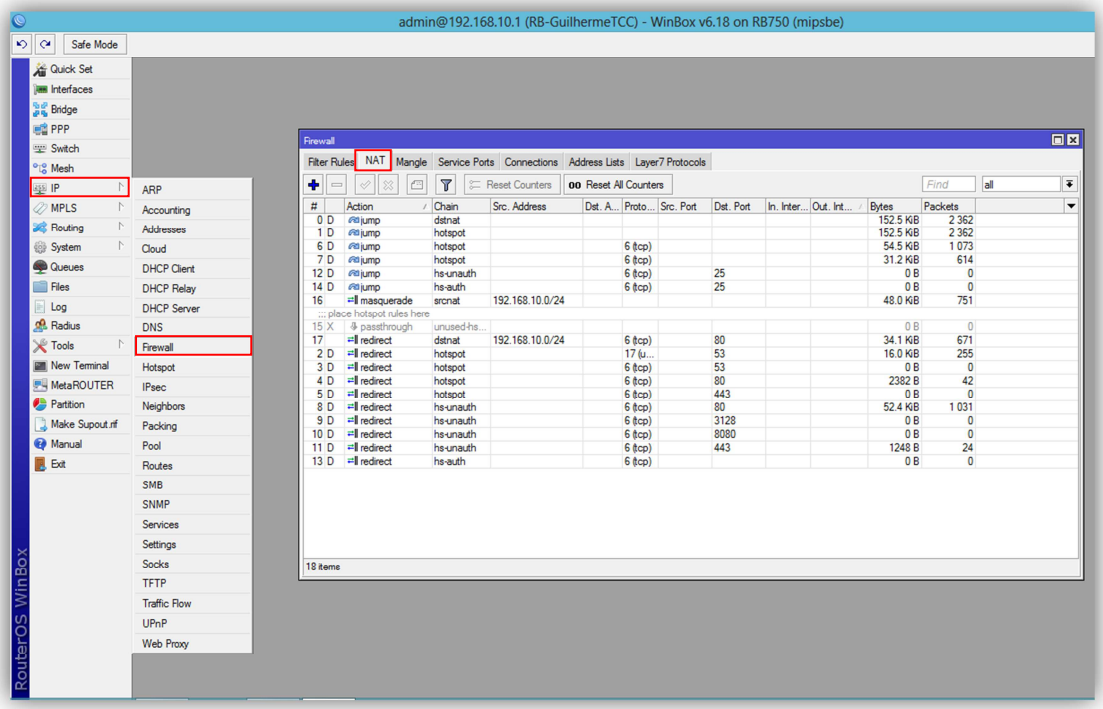


Imagem 62: NAT após a inclusão das regras pelo hotspot

11.6. TELA DE AUTENTICAÇÃO DO HOTSPOT

A partir de agora se tentarmos navegar na internet seremos redirecionados à tela padrão de autenticação do hotspot como na imagem abaixo. Essa tela solicitará as credenciais do cliente para que o hotspot efetue ou não a autenticação dele no servidor.

Nesse momento o nosso servidor hotspot já está em funcionamento.

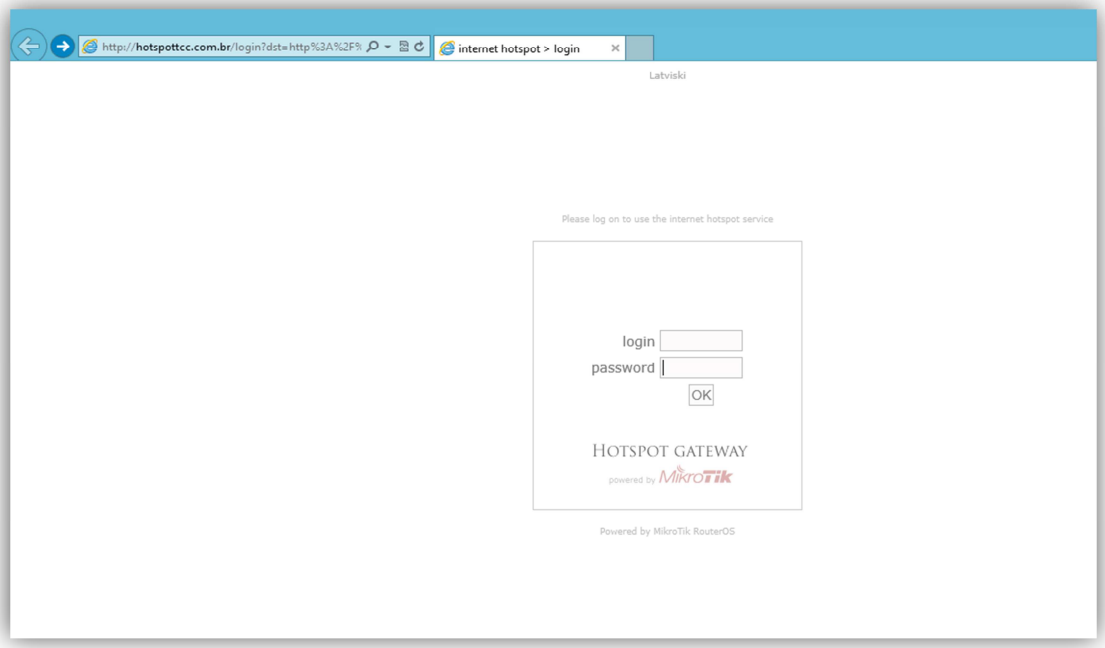


Imagem 63: Tela de solicitação de credenciais

Após preenchermos as credenciais na página de autenticação do hotspot com o usuário e senha admin criados anteriormente, somos autenticados no hotspot.

Como mostra a imagem abaixo entraremos no Menu: **IP=>Hotspot** e clicaremos na guia Active, essa tela nos mostra os usuários que estão autenticados no servidor hotspot no momento, qual o ip dado a ele**(address)**, quanto tempo ele está conectado**(Uptime)**, quanto tempo a conexão está ociosa(**Idle Time)** e quais são as taxas de upload**(RX Rate)** e download**(Tx Rate)** utilizadas no momento por cada usuário.

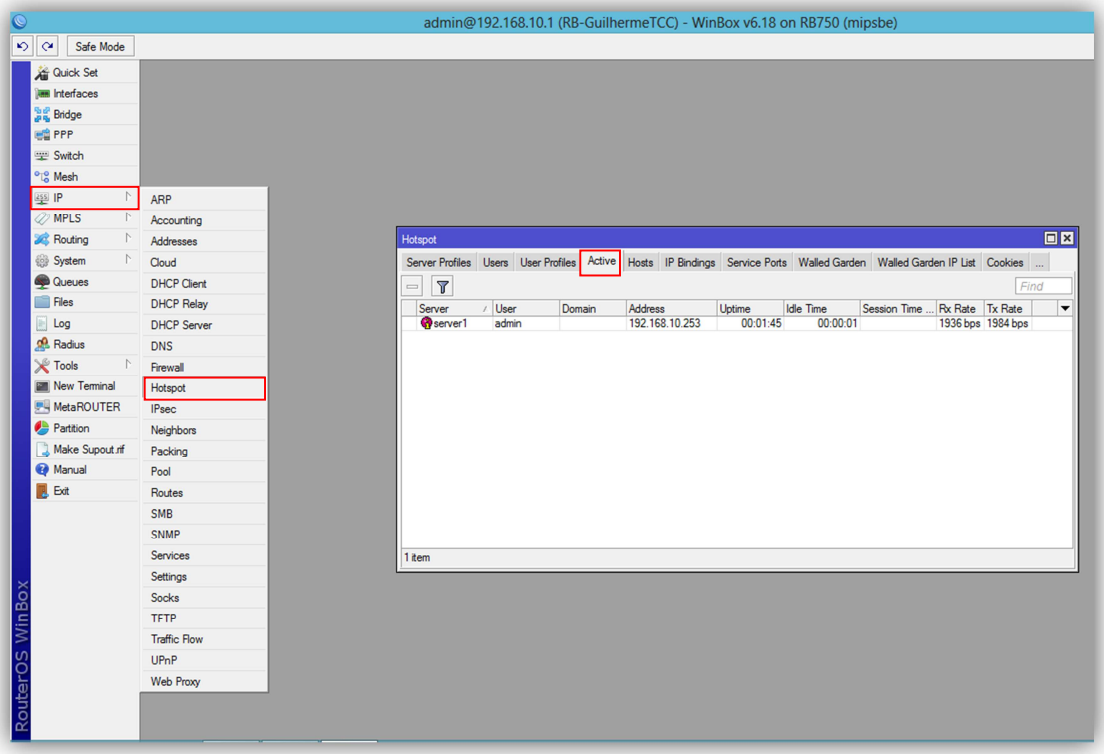


Imagem 64: Tela de usuários autenticados

11.7. IP BINDINGS, WALLED GARDEN E SIMPLE QUEUES

Depois de finalizada a configuração de nosso servidor hotspot vamos detalhar o funcionamento de três recursos do Hotspot, o IP Binding, o Walled Garden e o Simple Queues.

11.7.1. ADICIONANDO UMA REGRA DE IP BINDINGS

Uma das funcionalidades do IP Bindings é a liberação de um usuário específico da autenticação via usuário/senha ou usuário/MAC do servidor hotspot, sendo automaticamente autenticado ao se conectar na rede.

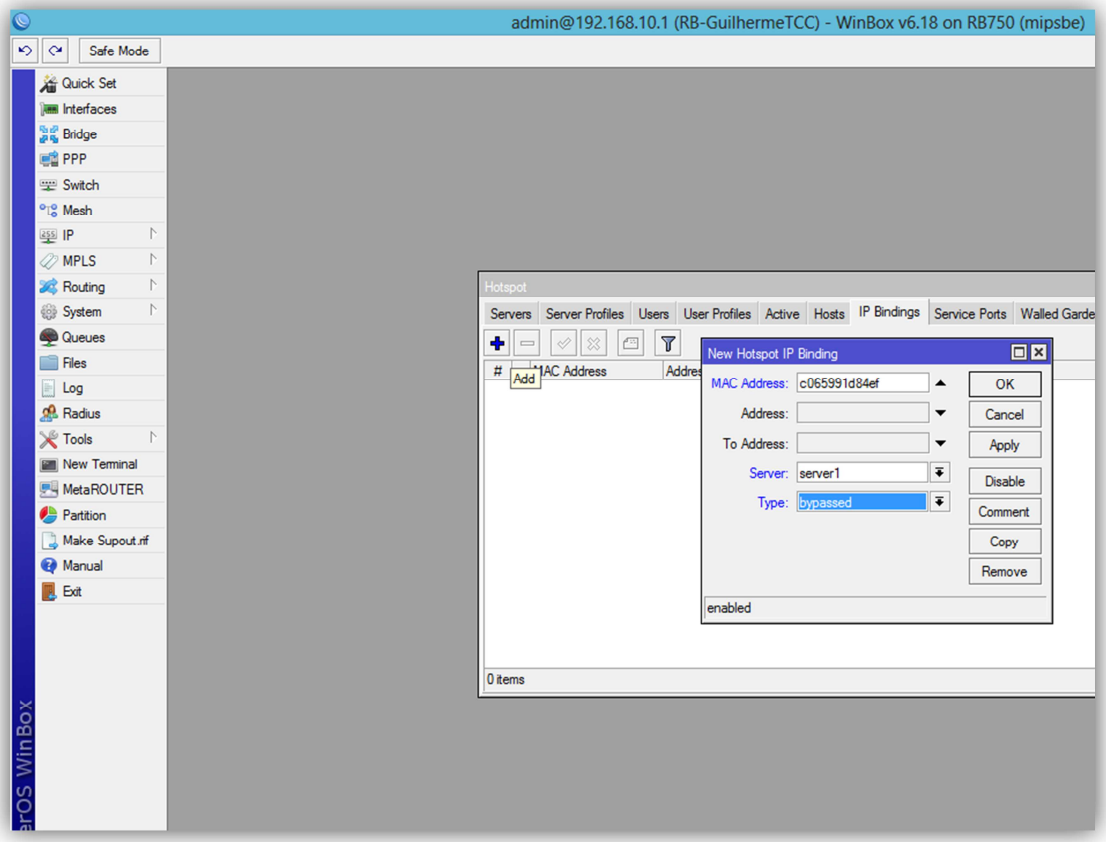


Imagem 65: Criação de regra IP Bindings

Agora iremos criar uma regra em que um usuário irá autenticar automaticamente sem precisar digitar as credencias na página de autenticação do hotspot, clicaremos na guia IP Bindigs e na tela inicial clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚, após isso será exibida a tela **New Hotspot IP Binding**, que é a tela de inclusão das regras, como mostra a Imagem65.

No campo **MAC Address** colocaremos o endereço MAC do microcomputador ou dispositivo do cliente que queremos que autentique automaticamente e no campo **Type** selecionaremos a opção bypassed, que permitirá o endereço contornar a autenticação do hotspot.

É possível também bloquear endereços para que não consigam autenticação somente alterando o campo **Type** para blocked em vez de bypassed, isso fará com que o endereço especificado não consiga autenticação no hotspot.

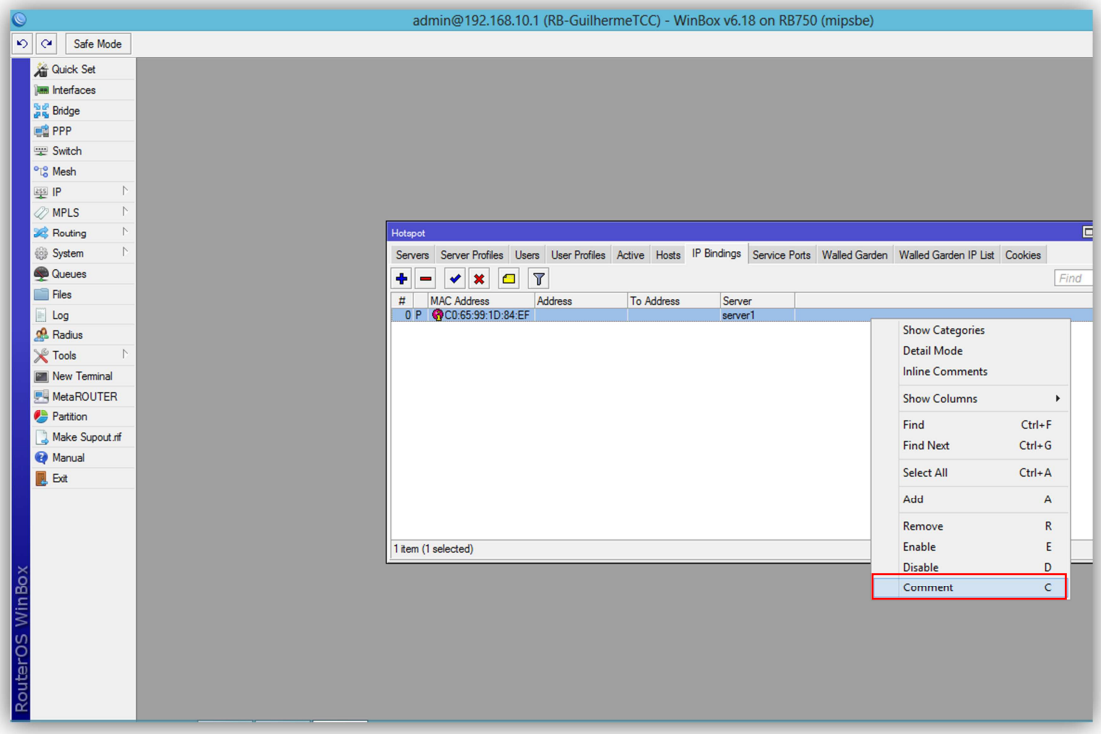


Imagem 66: Comentando uma regra no RouterOS

Uma dica importante para uma boa organização em nosso RouterOS é a identificação de nossas regras.

Clicaremos com o botão direito do mouse encima de uma regra escolheremos a opção **Comment** no menu, como na Imagem66.

Identificaremos a regra como Celular Guilherme, para que quando formos fazer alguma alteração nas regras nós saibamos o que significa essa regra e nesse caso específico do IP Bindings, a quem esse endereço MAC pertence.

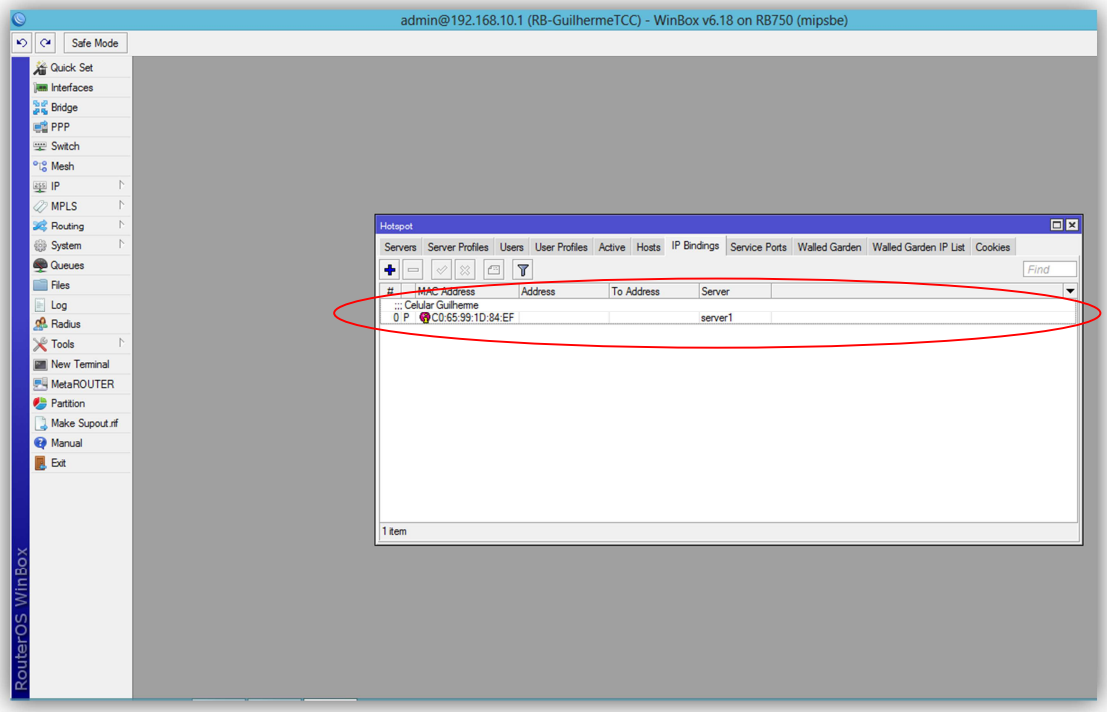


Imagem 67: Regra de IP Binding comentada

11.7.2. ADICIONANDO UMA REGRA DE WALLED GARDEN

Uma das funcionalidades do Walled Garden é a liberação da navegação de algum host específico mesmo sem a autenticação do usuário no hotspot.

Agora iremos criar uma regra que liberará a navegação de um site mesmo que os clientes não estejam autenticados, clicaremos na guia Walled Garden e na tela inicial clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida a tela **New Walled Garden Entry**, que é a tela de inclusão das regras, como mostra a Imagem68.

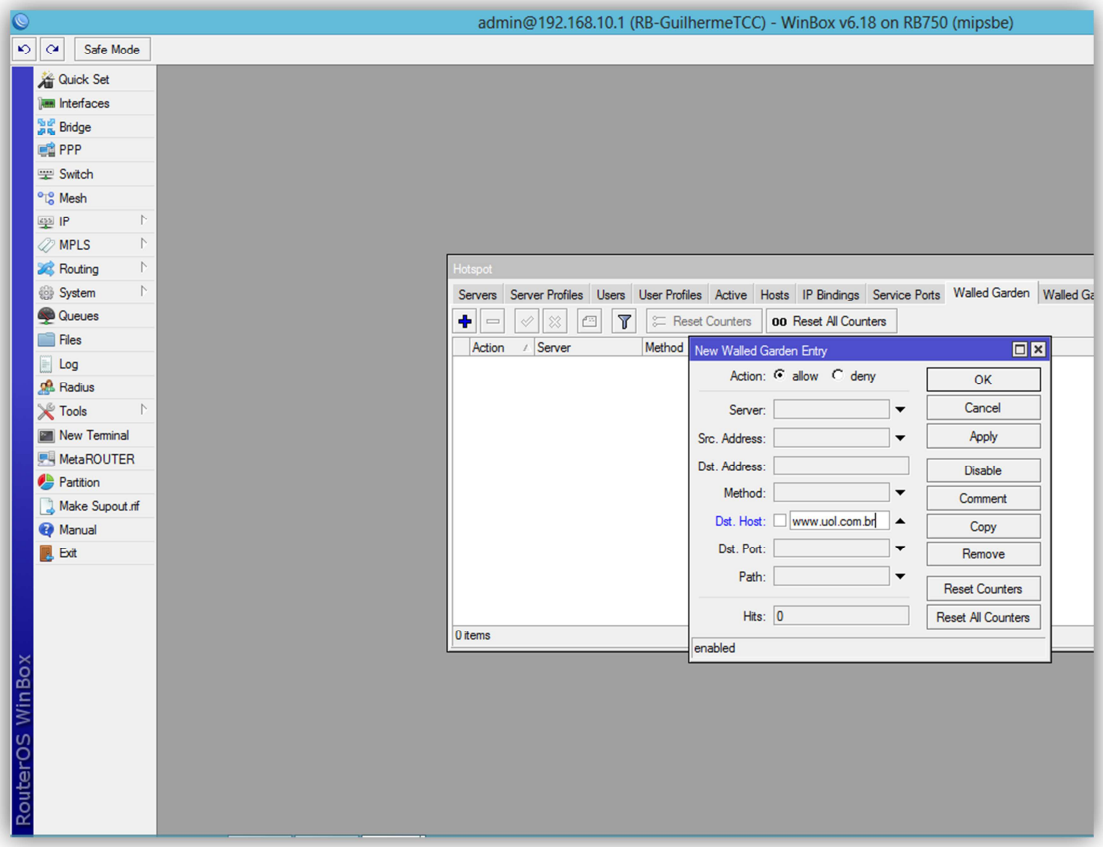


Imagem 68: Criação de regra Walled Garden

No campo **Action** selecionaremos a opção Allow, que irá liberar o acesso, no campo **Dst.Host** colocaremos o site que se deseja liberar a navegação mesmo o cliente não estando autenticado, nesse caso o site www.uol.com.br.

Os demais campos devem ficar no padrão do RouterOS, como na Imagem68.

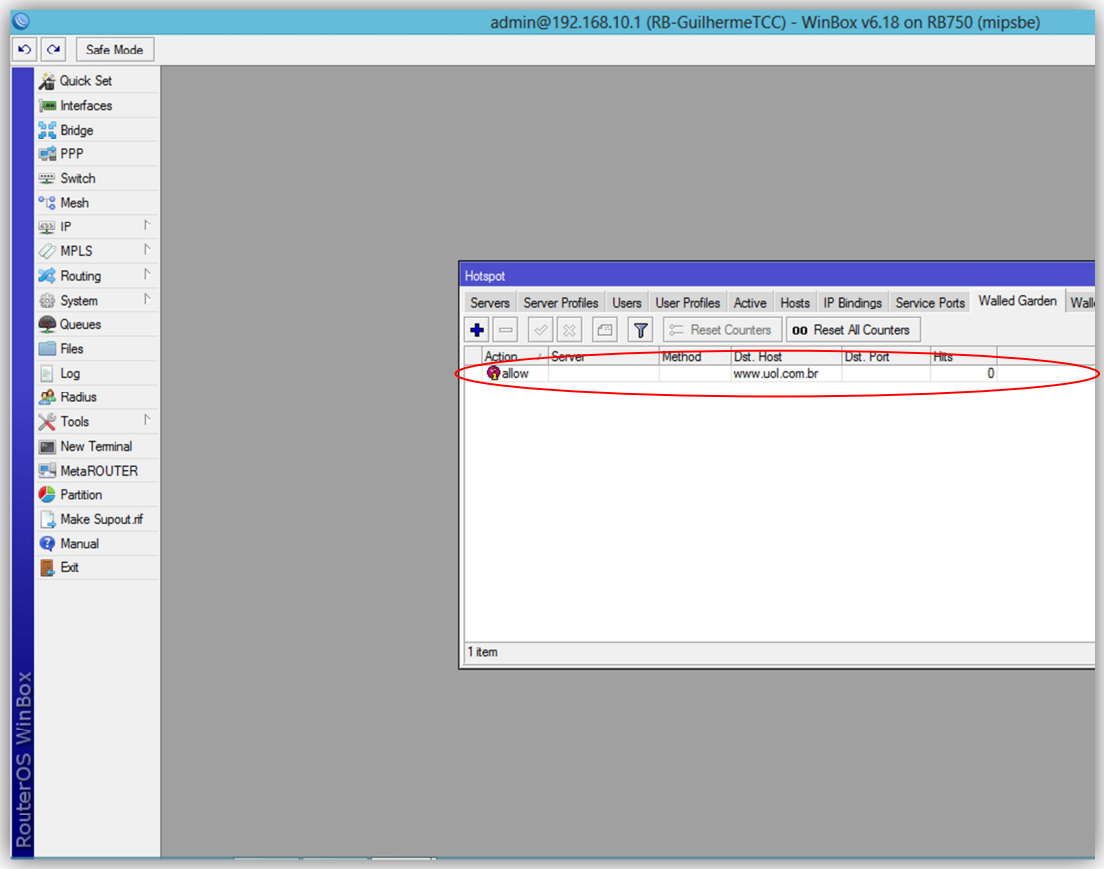


Imagem 69: Após a criação de regra Walled Garden

Essa regra fará que todo o tráfego de pacotes que o domínio de destino**(Dst.Host)** seja uol.com.br seja permitido(**Allow**) mesmo que o cliente não esteja autenticado no servidor.

11.7.3. SIMPLE QUEUES

No caso específico do Hotspot, o Simple Queues cria automaticamente uma regra de queue quando o usuário se autentica no servidor, baseado na regra de User Profile criada anteriormente, como mostra a imagem abaixo o hotspot criou uma regra de queue para o usuário admin dando 5M de upload e 5M de download para sua navegação.

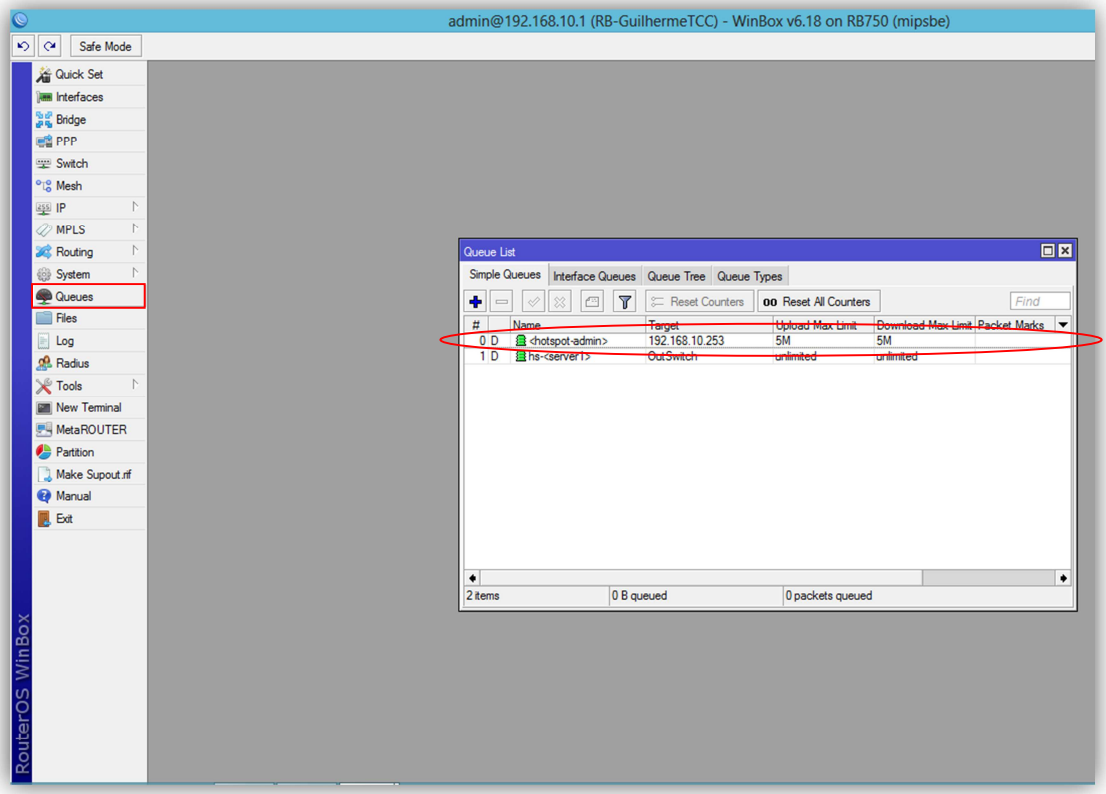


Imagem 70: Regras de Simple Queues

11.8. PERSONALIZANDO A TELA DE AUTENTICAÇÃO DO HOTSPOT

A tela de autenticação pode ser personalizada de acordo com a vontade do administrador do RouterOS ou da empresa responsável pelo servidor hotspot.

Como pode ser visualizado na Imagem abaixo, quando clicamos em Files o Winbox nos mostra uma árvore de diretório dos arquivos existentes em nossa Routerboard. Nessa árvore de diretórios podemos ver uma pasta com o nome de hotspot, nessa pasta estão os arquivos da página de autenticação, que podem ser personalizados.

Entre os vários arquivos, cada um com a sua finalidade destacamos o arquivo login.html que é o arquivo da página inicial de autenticação e por onde começa a personalização da área de autenticação.

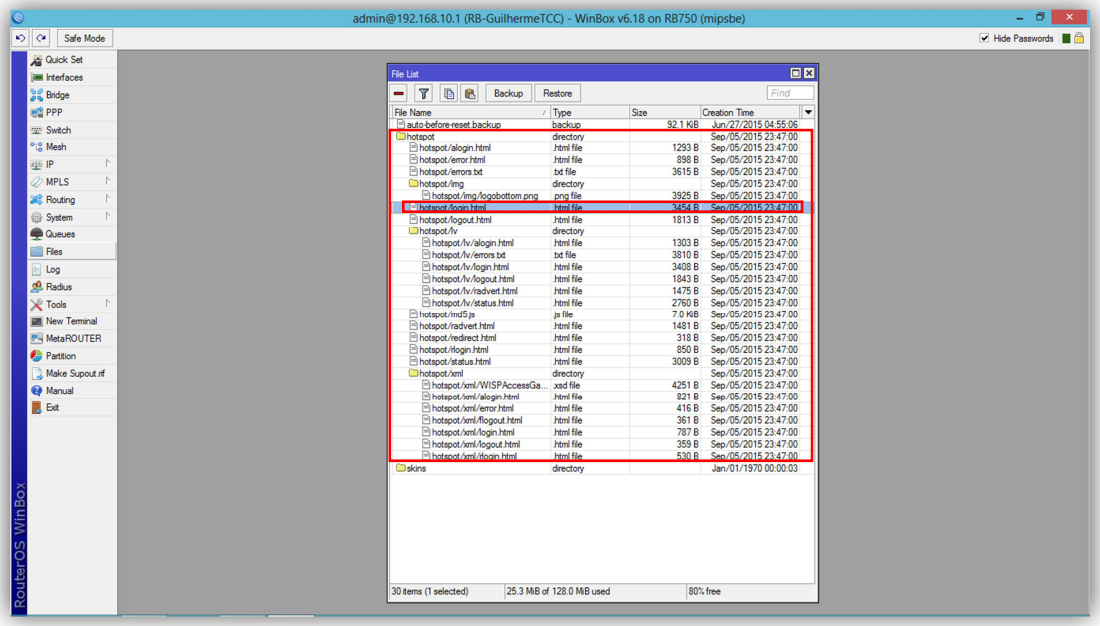


Imagem 71: Diretório de arquivos do RouterOS

Na imagem abaixo podemos visualizar uma página de autenticação do hotspot já personalizada.

Imagem 72: Exemplo de tela de autenticação personalizada

12. ALTERANDO A SENHA DO ROUTEROS

Para finalizar esse manual não podemos nos esquecer de fazer a alteração da senha de acesso padrão do administrador do RouterOS.

Para iniciar a troca da senha do administrador do RouterOS entraremos no Menu: **System=>Users**, em seguida daremos um duplo clique encima do usuário padrão existente em nosso RouterOS, o usuário admin.

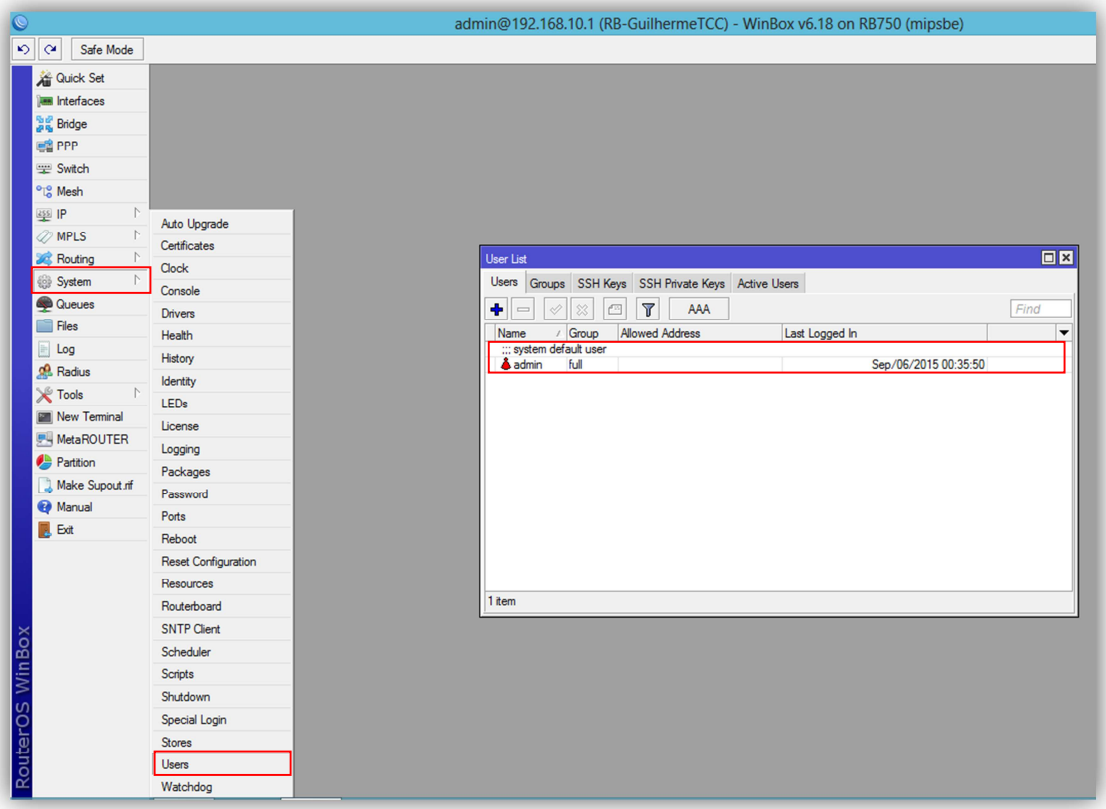


Imagem 73: User list do RouterOS

Será mostrada a tela de configuração do usuário admin, clicaremos então no botão Password .

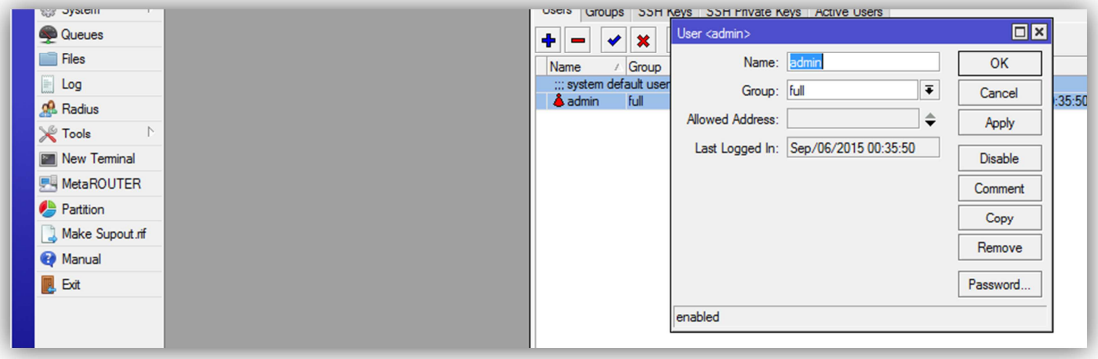


Imagem 74: Configuração do usuário admin

No campo **New Password** colocaremos a nova senha e confirmaremos a mesma senha no campo **Confirm Password**. Finalizaremos clicando em OK e seguida em OK novamente. A senha do administrador já está alterada.

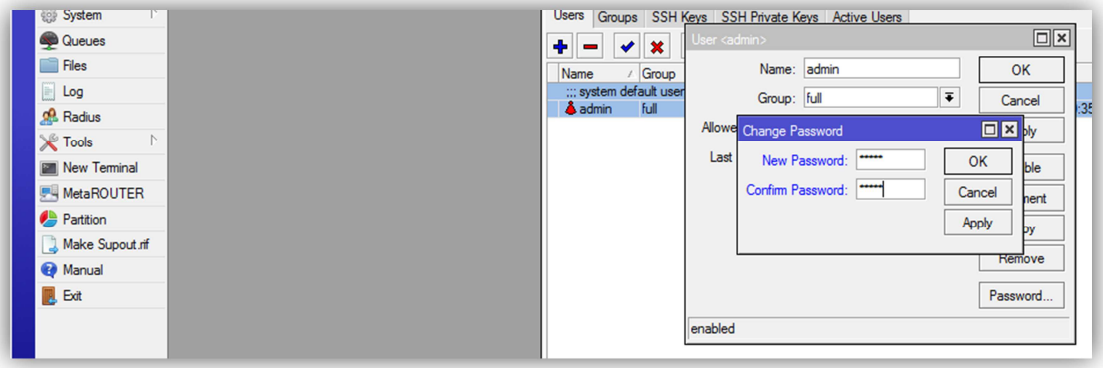


Imagem 75: Troca da senha do usuário admin

13. CONSIDERAÇÕES FINAIS

Esse manual se propôs, como objetivo principal, elaborar um conjunto de regras e procedimentos para facilitar a criação e configuração de um servidor Hotspot no sistema operacional RouterOS de um modo correto e otimizado, e assim, oferecer condições de utilização adequada desse hotspot aos usuários e ao administrador.

Espero que esse manual ajude e potencialize o processo de criação e configuração do servidor.

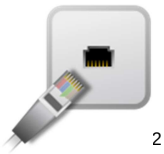
14. REFERÊNCIAS

MIKROTIK.com. Site Oficial
Disponível em:http://www.mikrotik.com/pdf/what_is_routeros.pdf/> Acesso em: 05 set.2015.

Imagem cabeçalho 01

[1]

Imagem cabeçalho 02


[2]

[1] Disponível em: http:// www.marceloinformatica.net.br/;. Acesso em 06 Set. 2015.
[2] Disponível em: http://icones.pro/en/emblem-shared-ethernet-png-image.html;. Acesso em 06 Set. 2015.