



GUIA EXCLUSIVO DE REFERÊNCIA



HOTSPOT



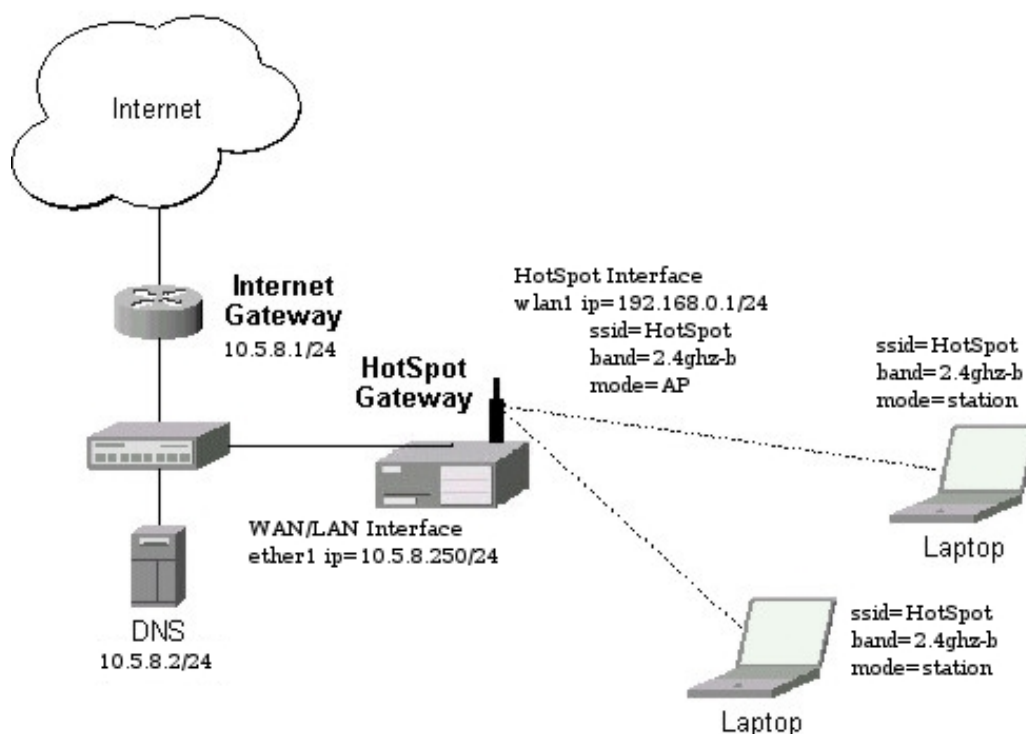
HOTSPOT

Hotspot é um termo utilizado para se referir a uma área pública onde está disponível um serviço de acesso a Internet, normalmente através de uma rede sem fio Wi-Fi. Aplicações típicas incluem o acesso em Hotéis, Aeroportos, Shoppings, Universidades, etc.

O conceito Hotspot pode ser usado, no entanto, para dar acesso controlado a uma rede qualquer, com ou sem fio, através de autenticação baseada em nome de usuário e senha.

Quando em uma área coberta por um Hotspot, um usuário que possua um Laptop e tente navegar pela WEB é arremetido para uma página do Hotspot que pede suas credenciais, normalmente usuário e senha. Ao fornecê-las e sendo um cliente autorizado pelo Hotspot o usuário ganha acesso à internet, podendo sua atividade ser controlada e bilhetada.

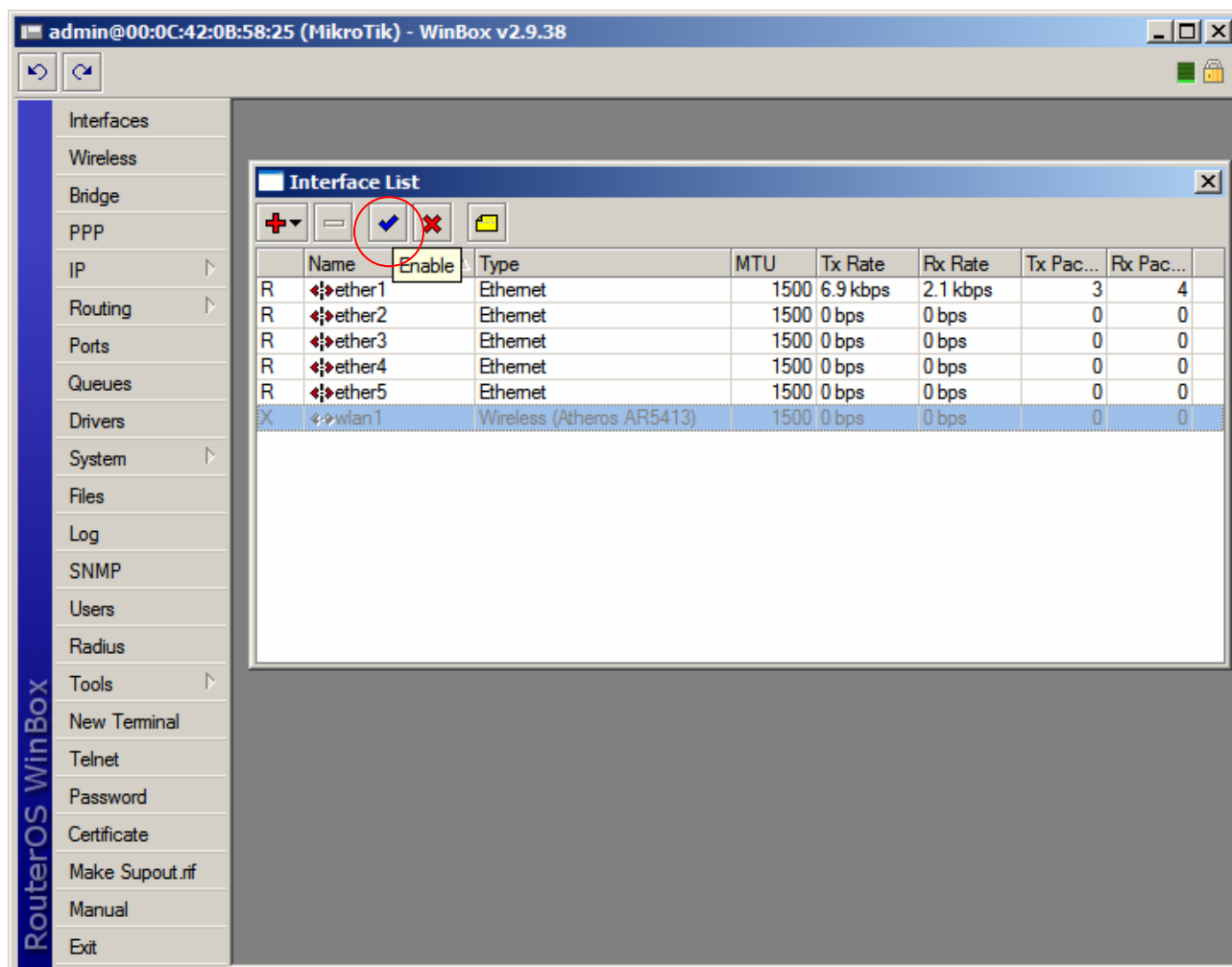
Considerando a estrutura da imagem abaixo:





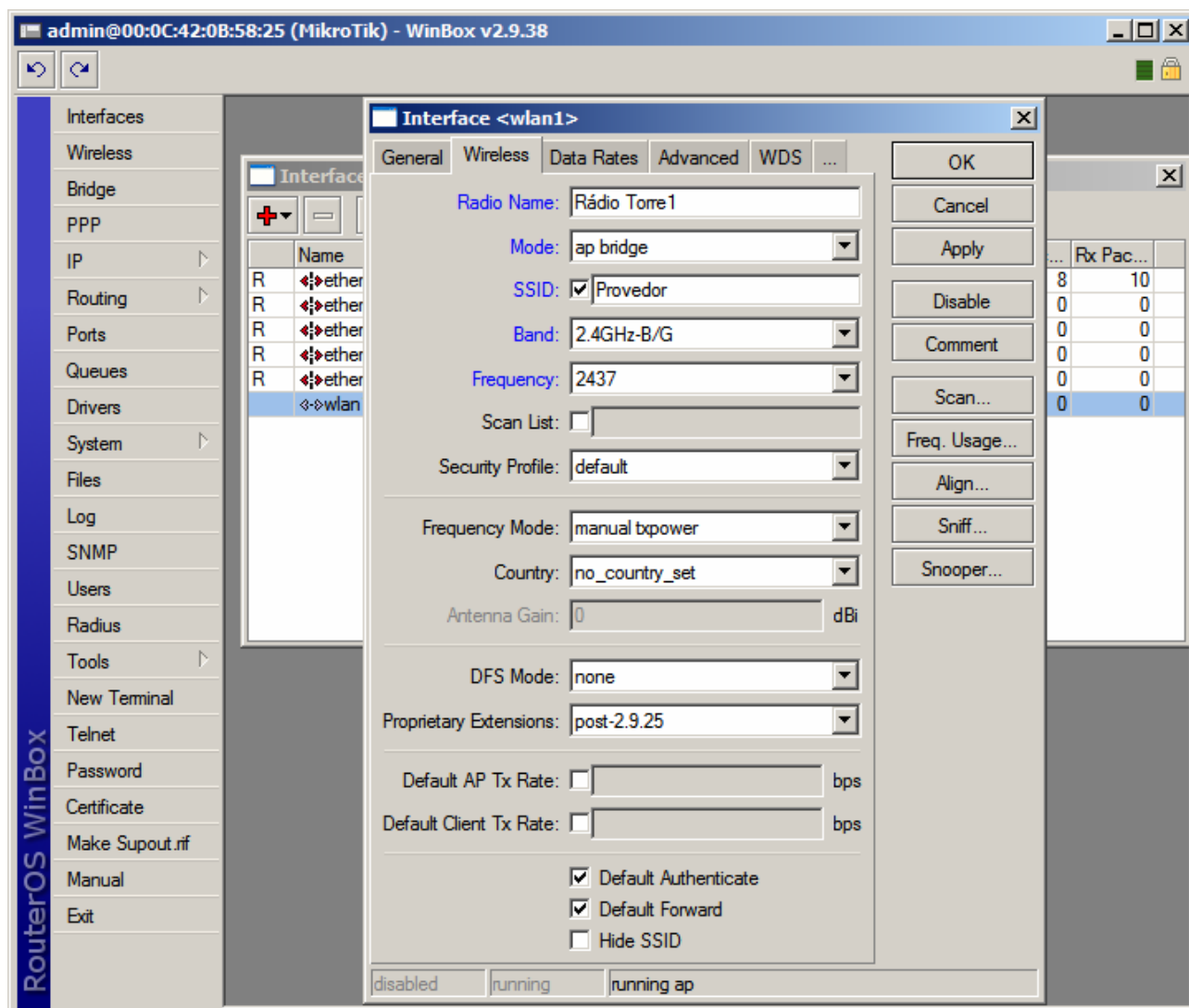
Primeiramente devemos habilitar as interfaces e configurar a interface que será o hotspot.

- Clique no menu Interfaces.
- Clique na interface Wlan desejada e clique no botão Habilitar





- Dê um clique duplo na interface habilitada
- Na guia Wireless, configure as opções:
- Opção "Radio Name": Coloque nessa opção o nome que você deseja que o Rádio tenha na rede.
- Opção "Mode": AP Bridge
- Opção "Band": Escolha a Banda de Operação desejada
- Opção "Frequency": Canal de operação do equipamento
- Clique no botão "OK"

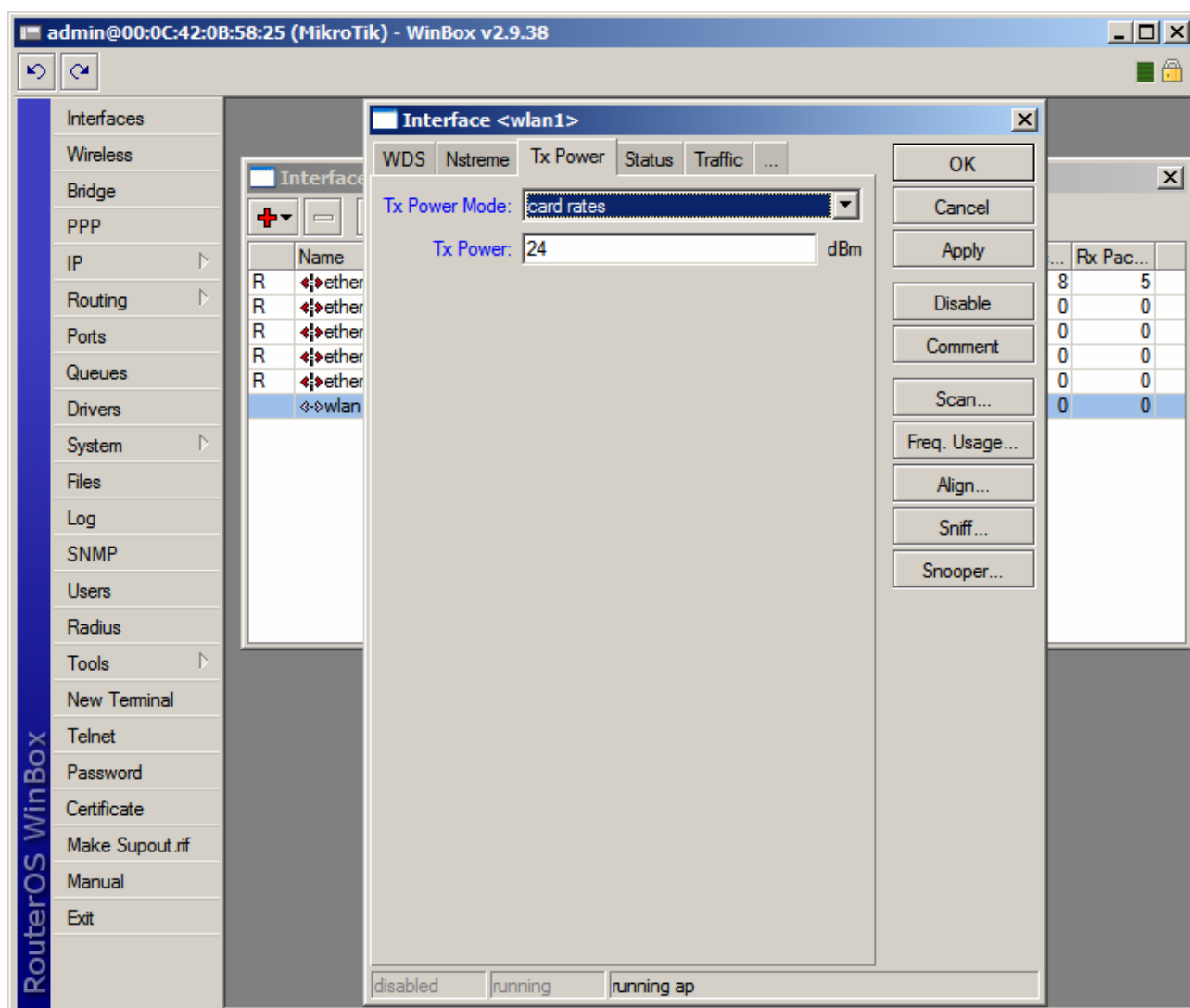




- Clique na guia “Tx Power” para escolher a potência do cartão, considerando:

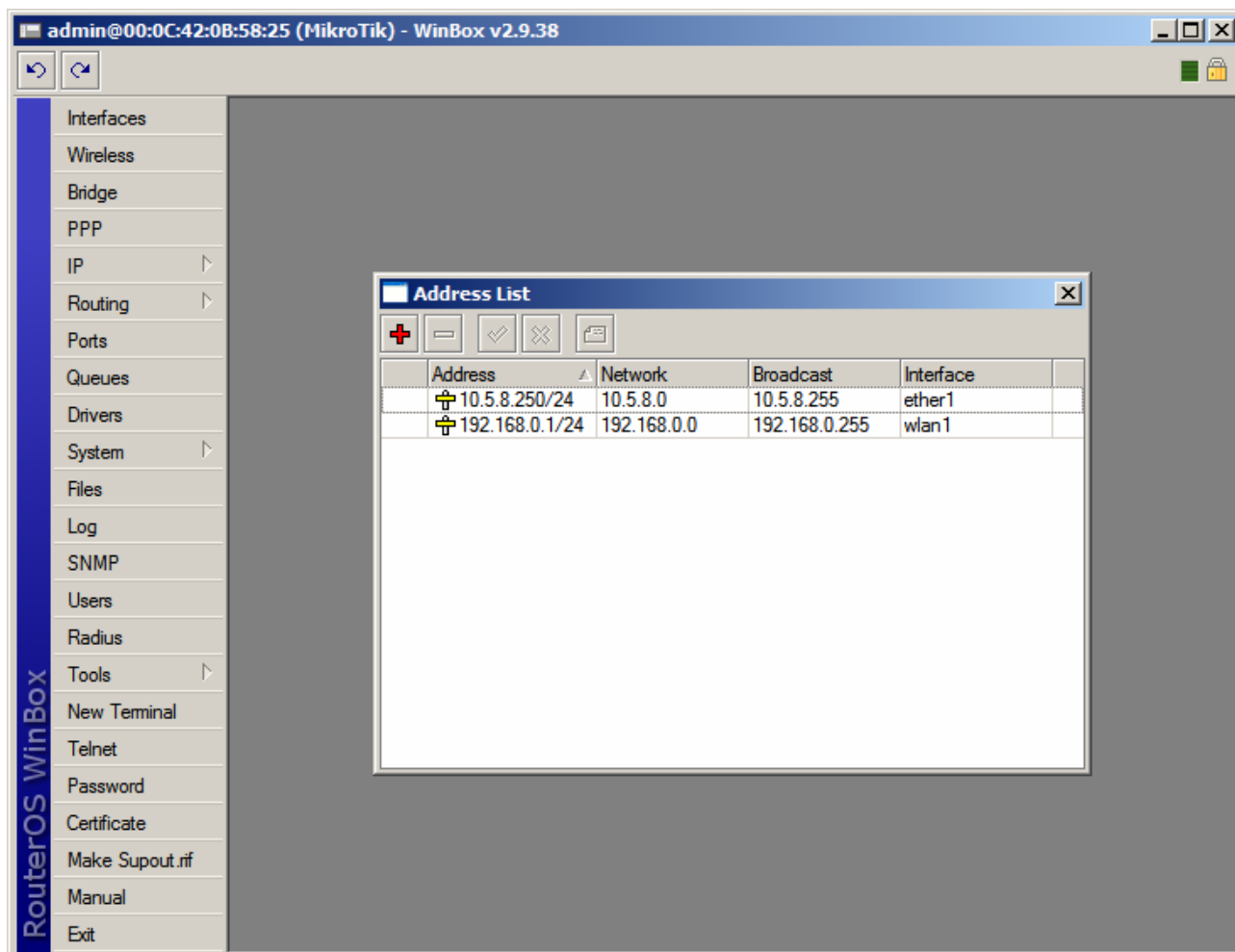
17dBm	=	50mW (default)
18dBm	=	63mW
20dBm	=	100mW
22dBm	=	150mW
23dBm	=	200mW
24dBm	=	250mW
25dBm	=	316mW
26dBm	=	400mW

Obs: Verifique a potência máxima permitida para o cartão utilizado antes de fazer a alteração.





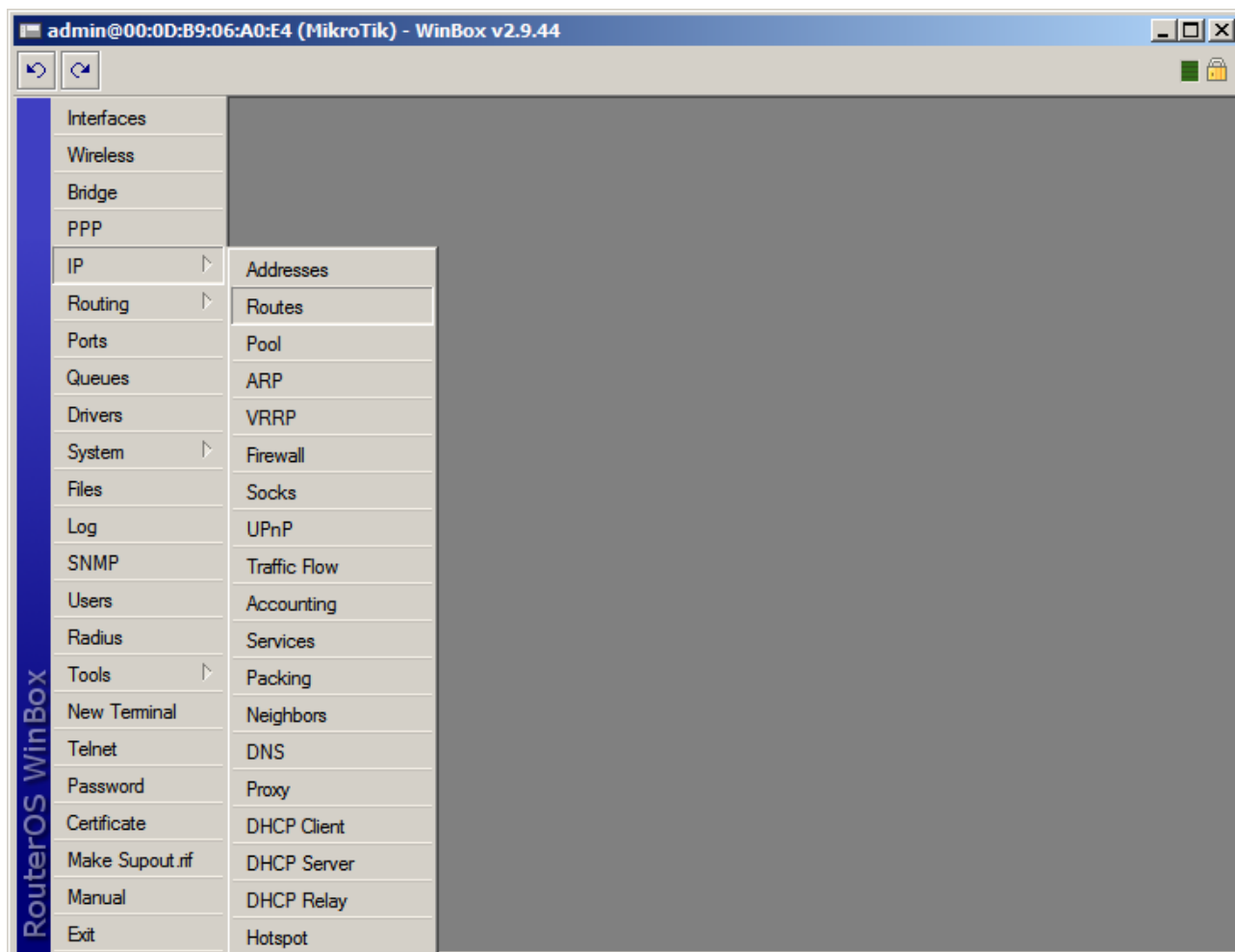
Devemos configurar os IPs para as suas respectivas interfaces:





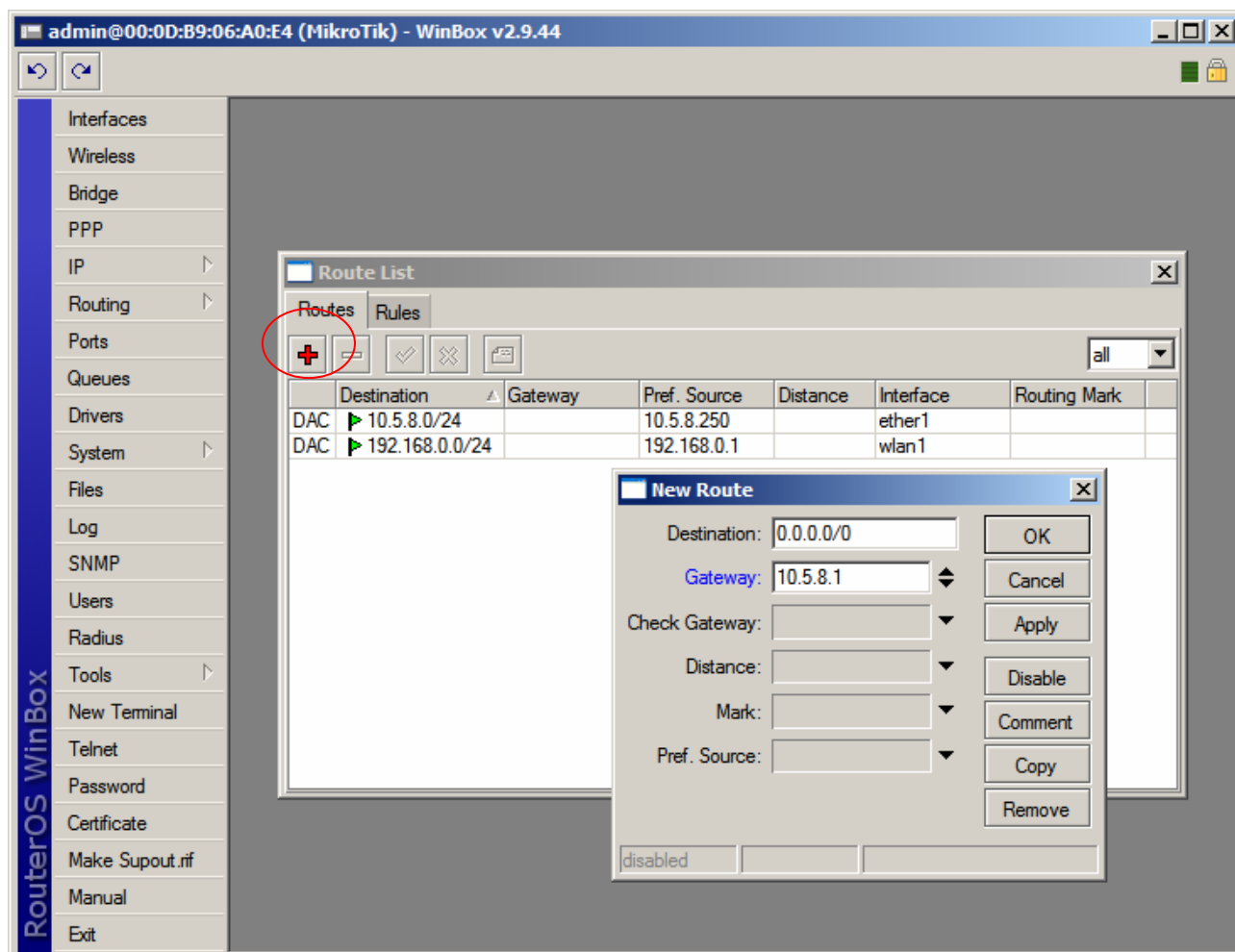
Devemos definir o Gateway de saída para a internet

- Clique no menu "IP"
- Clique na opção "Routes"



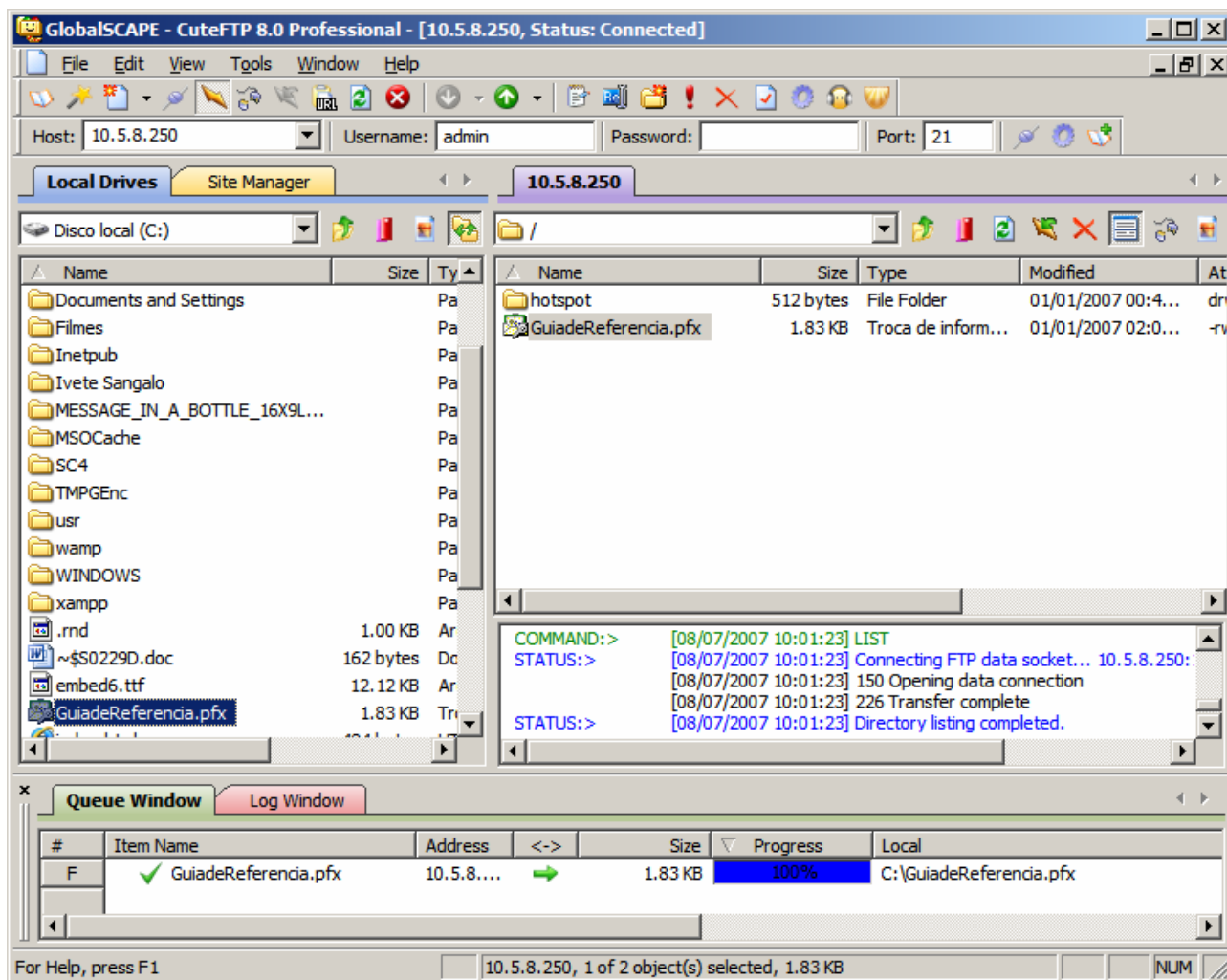


- Clique em “Adicionar”
- No campo “Gateway”, digite o IP do servidor Gateway.
- Clique no botão “OK”





Se você possuir um Certificado de Segurança, faça a transferência dele para o Mikrotik através de FTP, utilizando qualquer cliente de FTP:



O QUE É SSL?

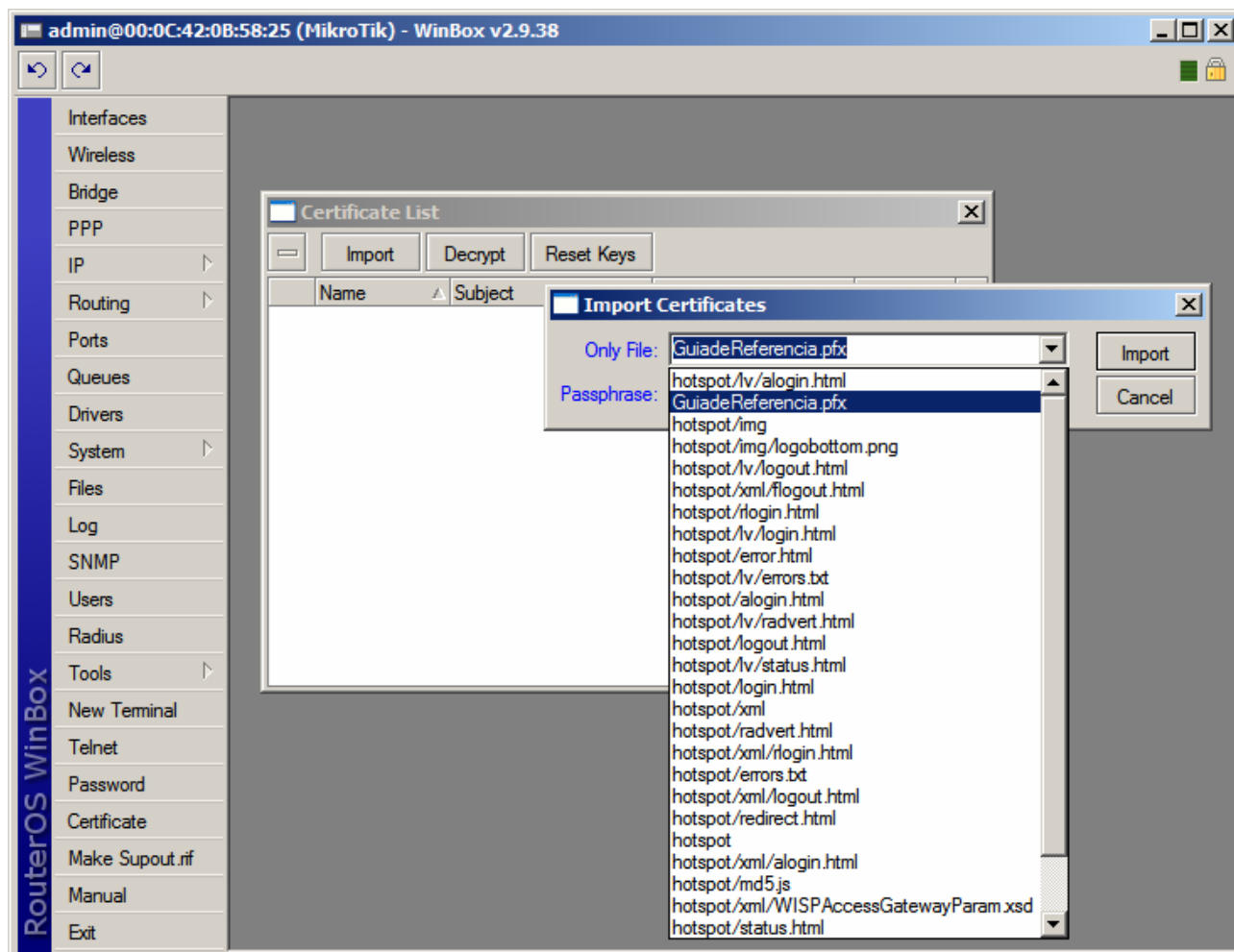
SSL (Secure Sockets Layer) é uma tecnologia de segurança que é comumente utilizada para codificar os dados trafegados entre o computador do usuário e o um website. O protocolo SSL, através de um processo de criptografia dos dados, previne que os dados trafegados possam ser capturados, ou mesmo alterados no seu curso entre o navegador (browser) do usuário e o site com o qual ele está se relacionando, garantindo desta forma informações sigilosas como login e senha, neste nosso caso.

Uma sugestão: Pode-se contratar um Certificado de Segurança através do site: <http://www.laniway.com.br/br/corporativo/certificado.do.jsessionid=441CFD641B6F5981DE6594BF96E3D5FD>



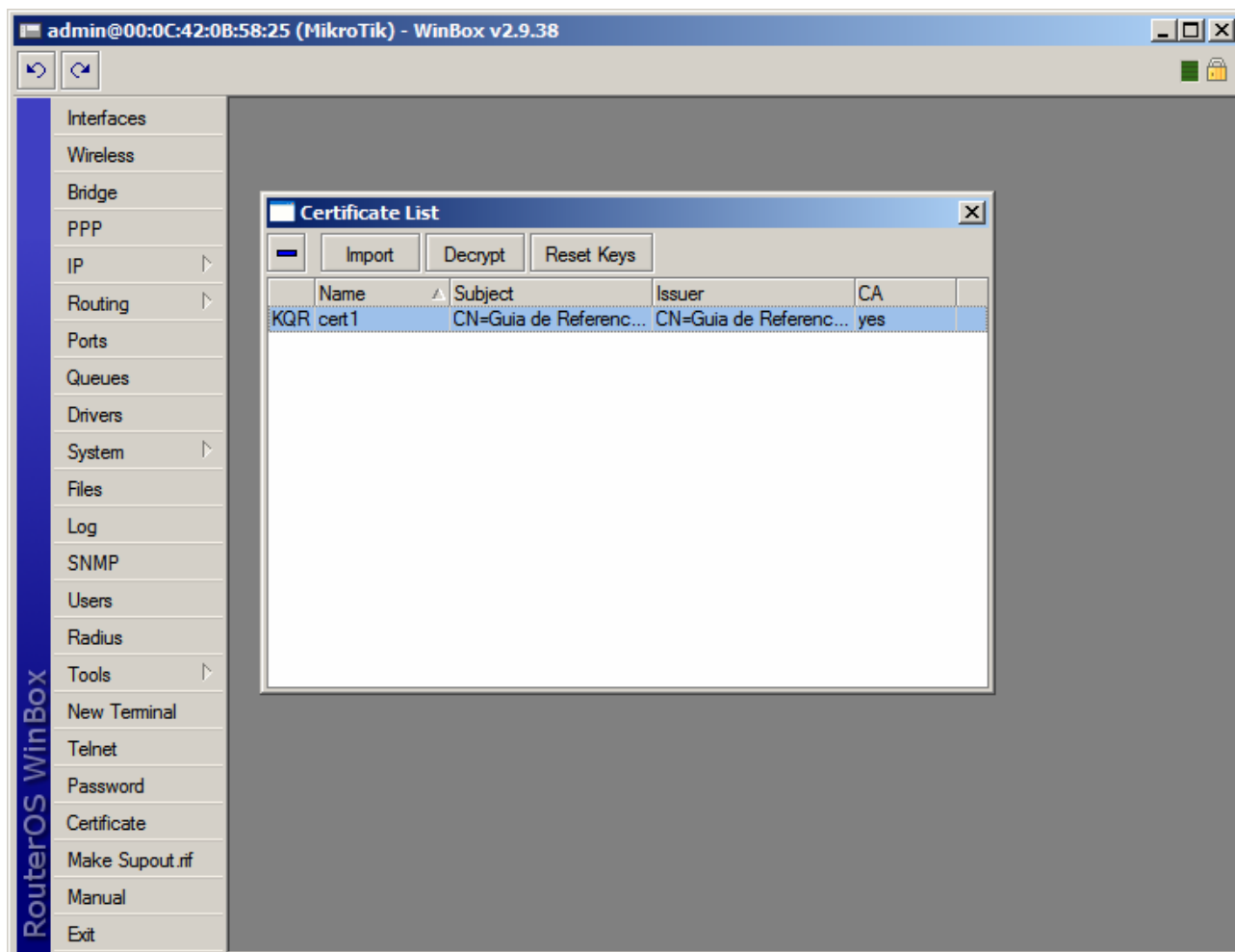
O próximo passo será fazer a importação do Certificado

- Clique no menu "Certificate"
- Clique no botão "Import"
- Na opção "Only File", escolha o Certificado que você transferiu anteriormente.
- Na opção "Passphrase", digite a senha do seu Certificado
- Clique no botão "Import"





Seu Certificado estará importado



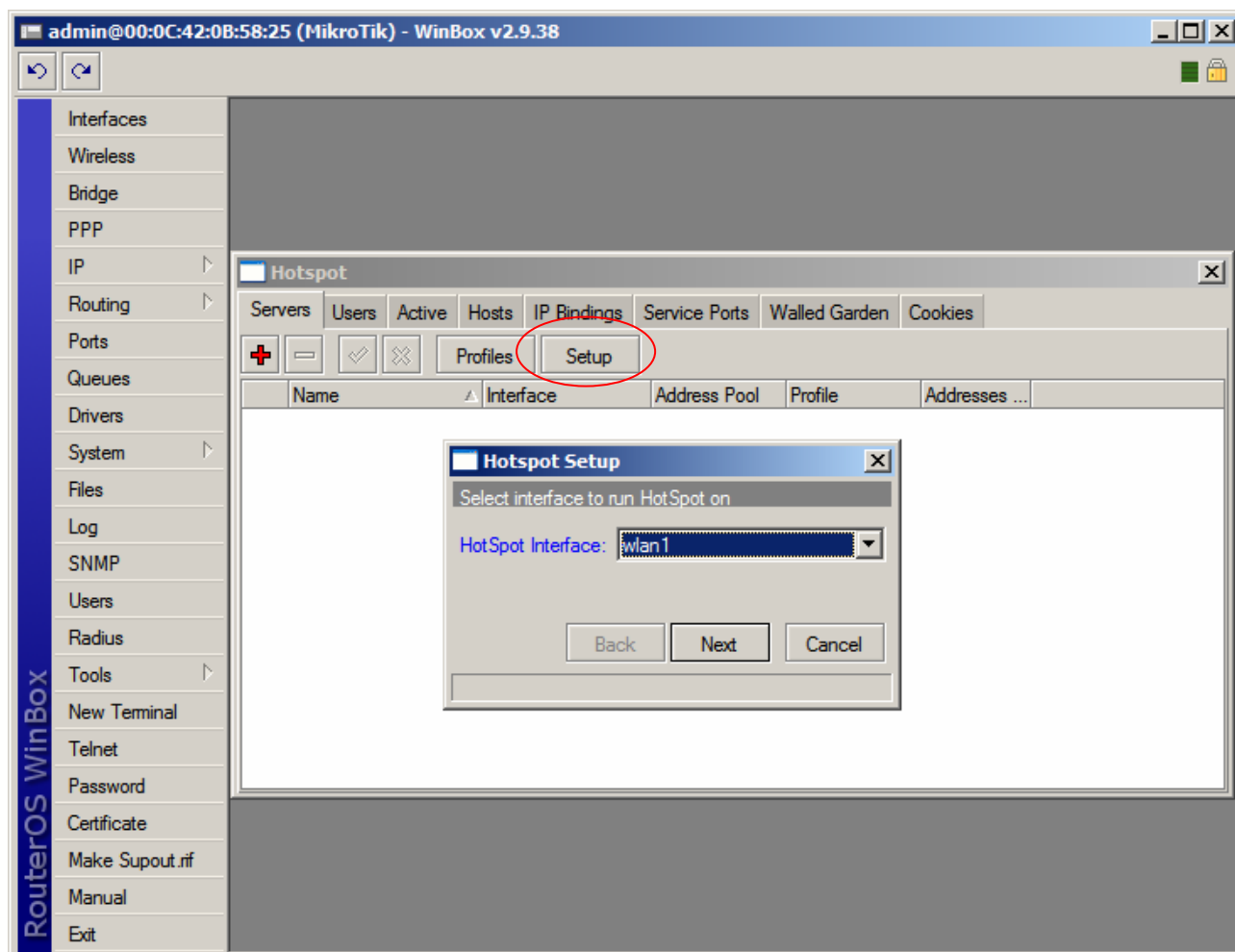


- Clique no menu “IP”
- Clique na opção “Hotspot”



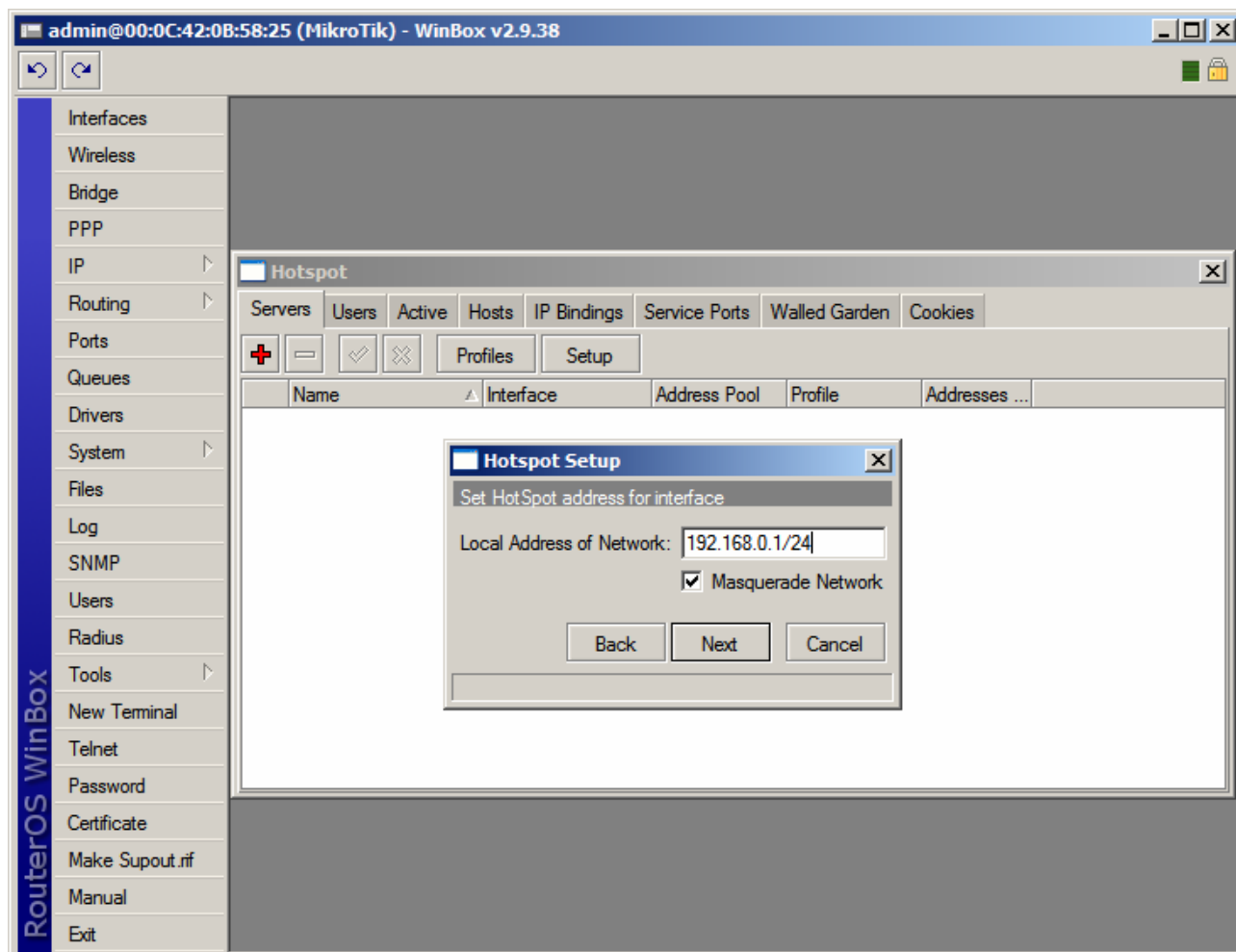


- Clique no botão "Setup"
- Selecione a interface onde os clientes se conectarão ao Hotspot.
- Clique no botão "Next"



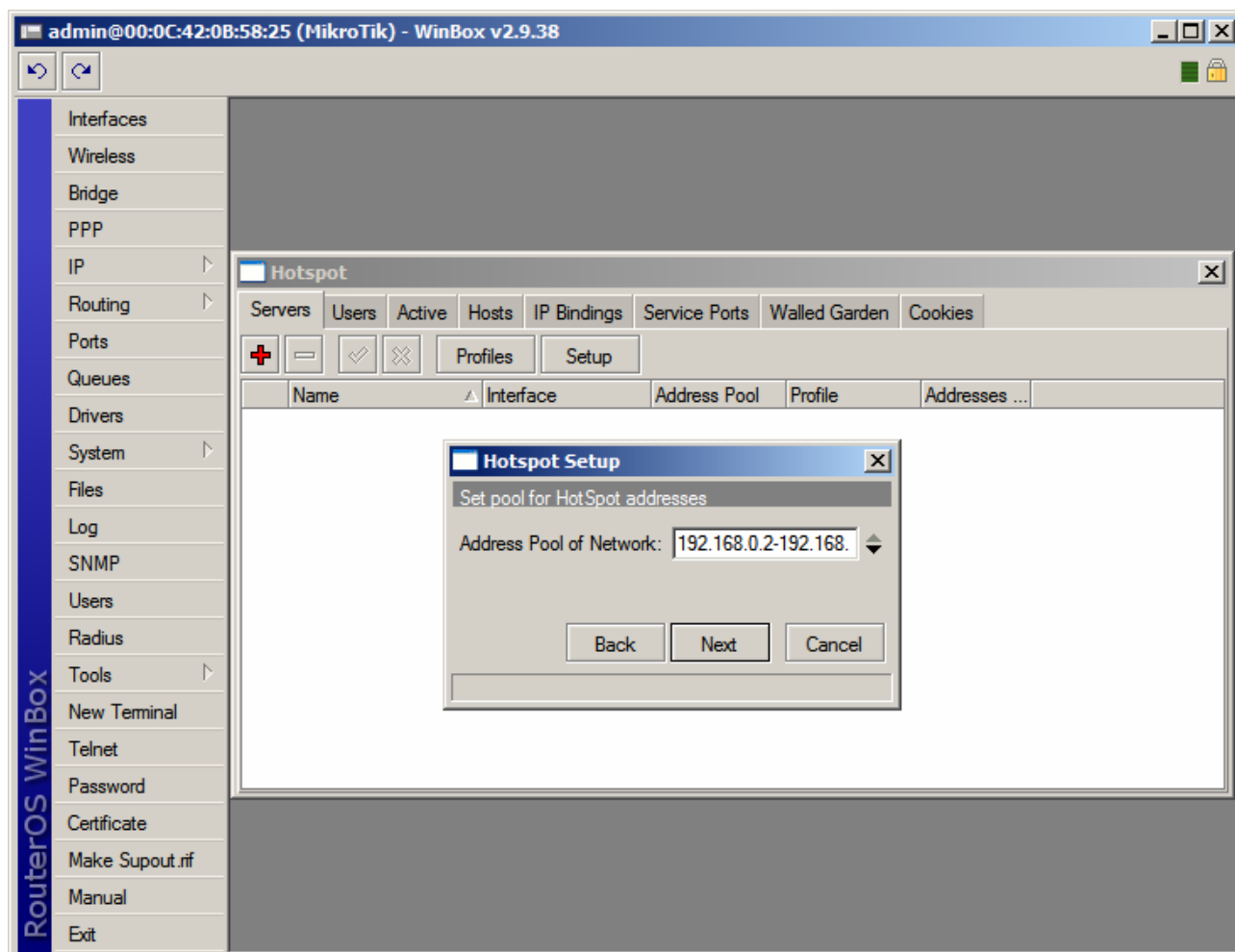


- No campo "Local Address of Network" aparecerá o IP da interface escolhida.
- Clique no botão "Next"



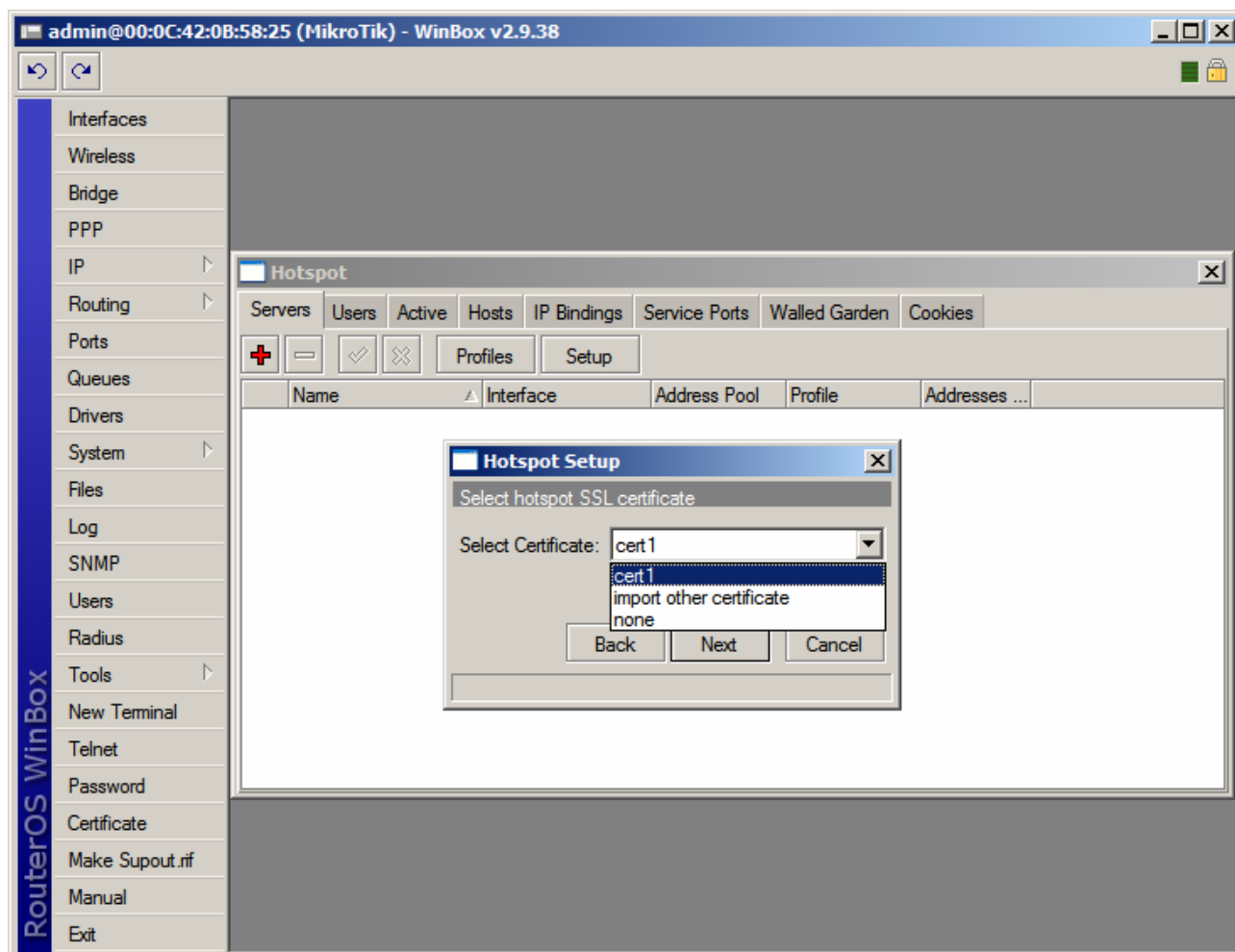


- No campo “Address Pool of Network” aparecerá o pool dos IPs que serão distribuídos aos clientes. Em nosso exemplo, é sugerido pelo Mikrotik o pool: 192.168.0.2-192.168.0.249
- Clique no botão “Next”



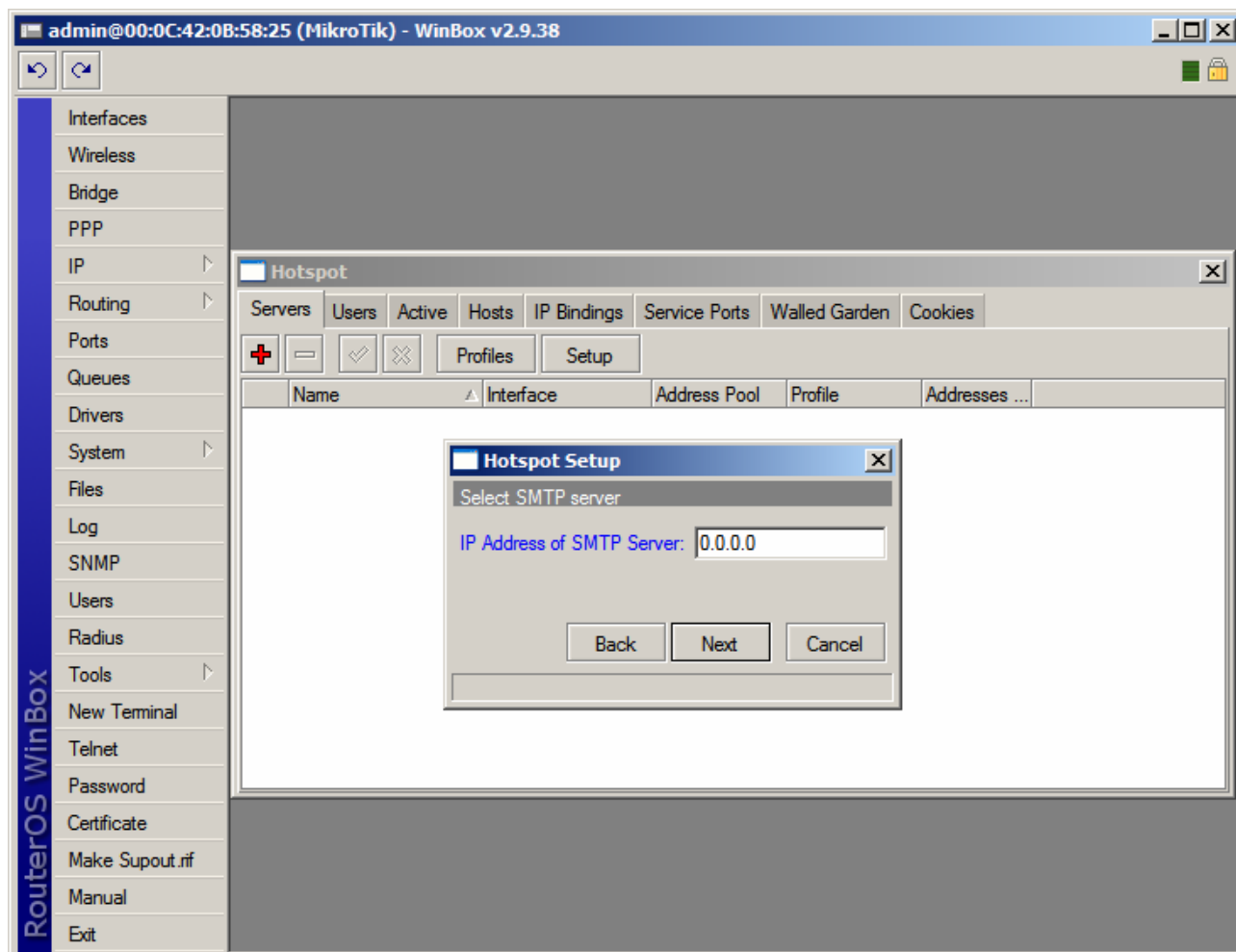


- Na opção "Select Certificate" escolha o certificado importado anteriormente. Caso você não tenha nenhum certificado, escolha a opção "none".
- Clique no botão "Next"



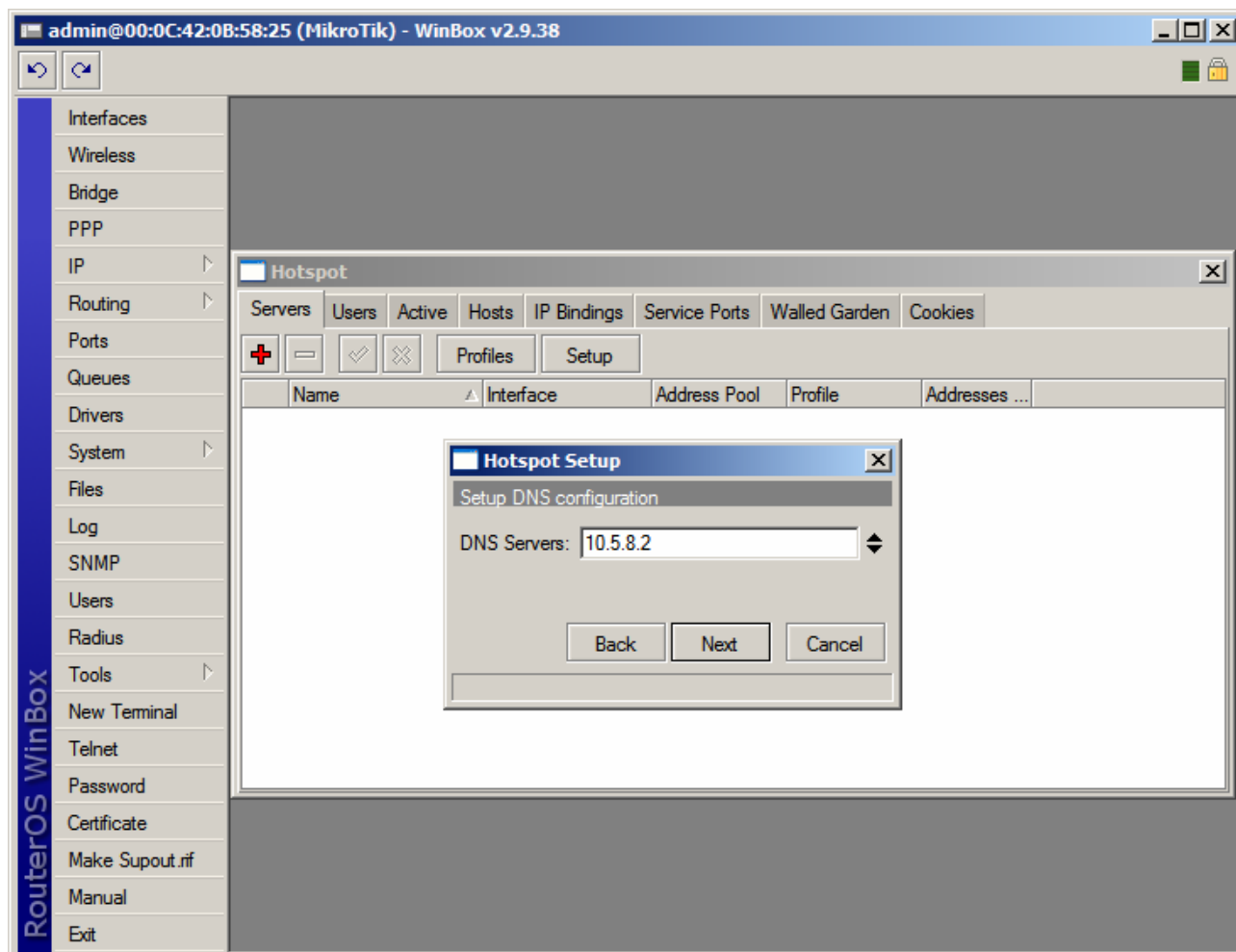


- Na opção "IP Address of SMTP Server", digite o IP de seu Servidor SMTP, se desejar.
- Clique no botão "Next"



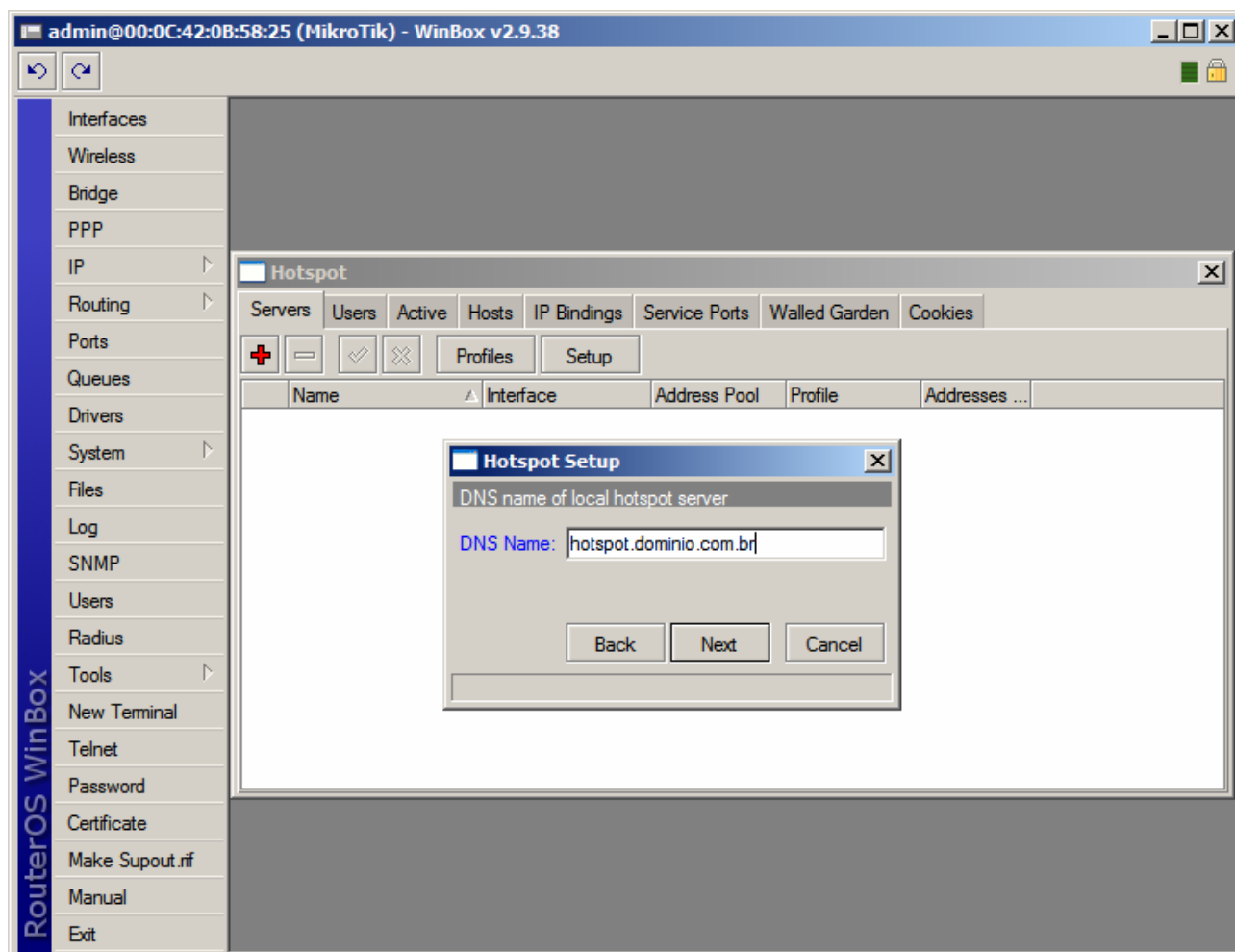


- Na opção “DNS Servers” digite o IP do seu servidor DNS.
- Clique no botão “Next”



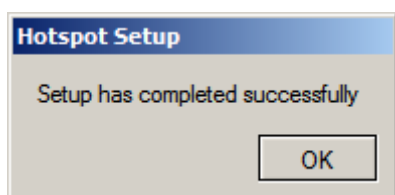
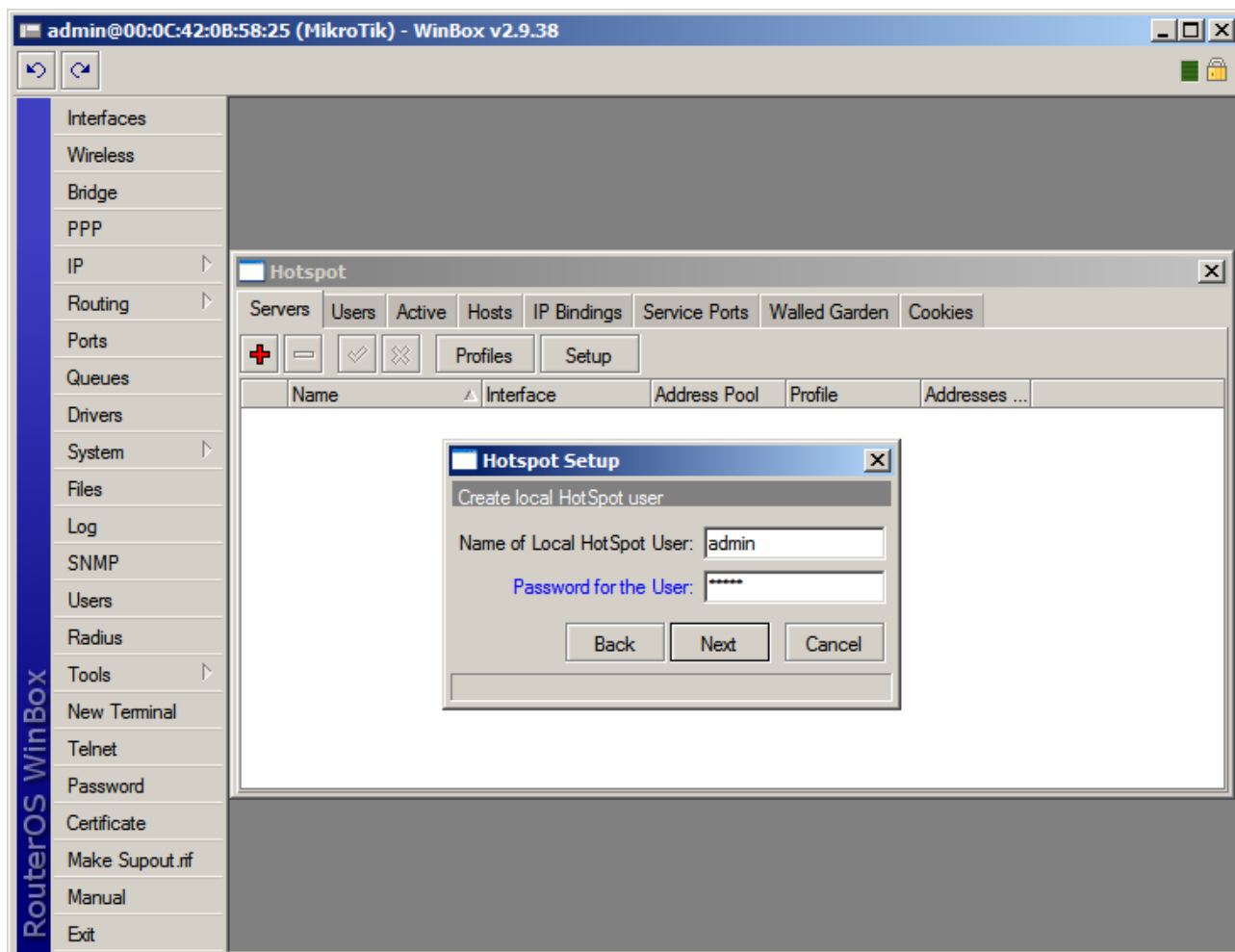


- Na opção “DNS Name”, Dê o nome do DNS (aparecerá no Browser dos clientes ao invés do IP).
- Clique no botão “Next”





- Na tela seguinte, por default, é cadastrado o usuário Administrador (admin).
- Após o cadastro, clique no botão "Next"

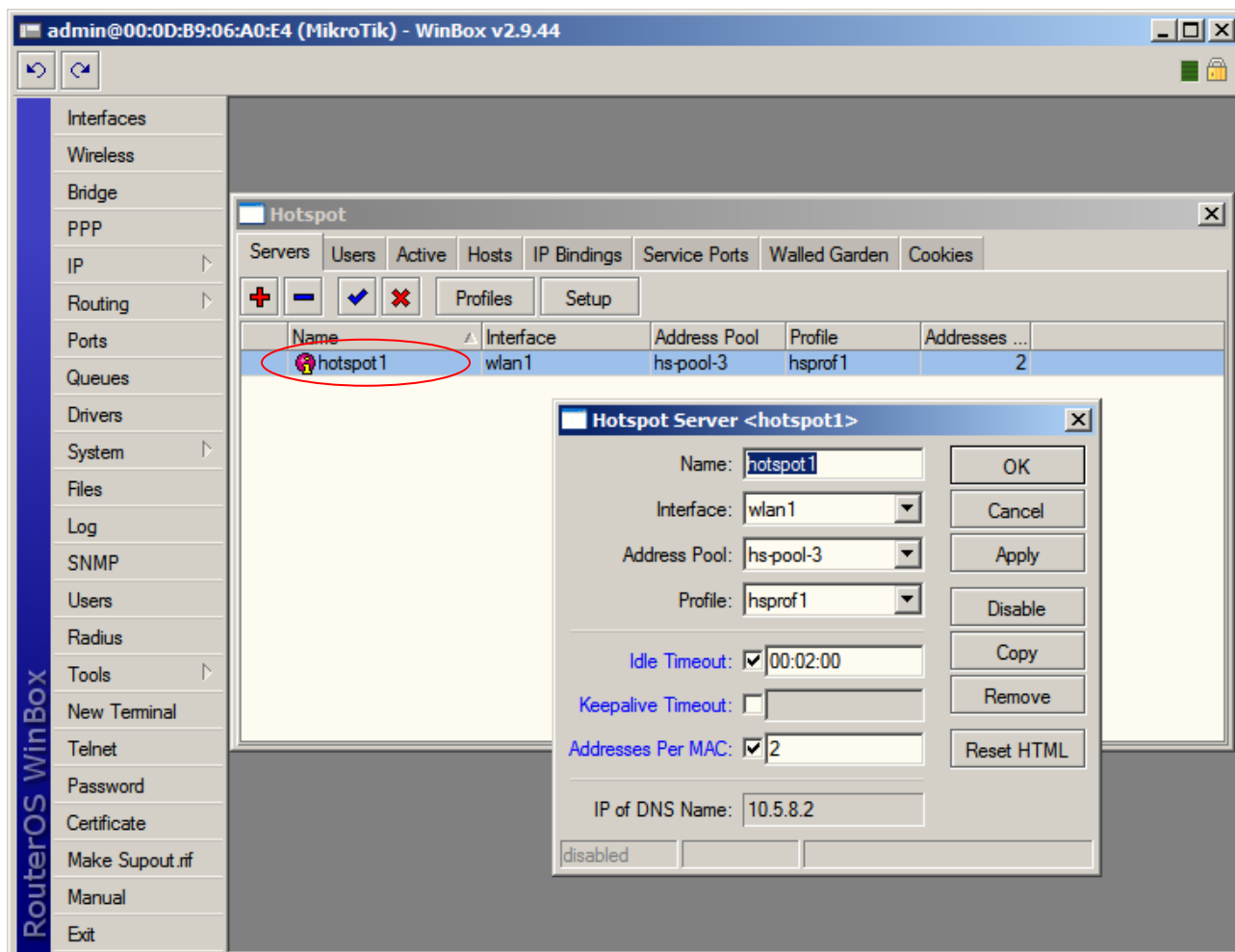


Seu Hotspot está configurado.

Embora tenha sido uma configuração fácil e rápida, o Mikrotik se encarregou de fazer o trabalho pesado, criando as regras apropriadas no Firewall, bem como uma fila específica para o Hotspot.



DETALHES DA CONFIGURAÇÃO



- idle Timeout (time | none; default: none)

Máximo período de inatividade para clientes autorizados. É utilizado para detectar quais clientes não estão usando redes externas (internet) e que não há tráfego do cliente através do roteador. Atingindo o timeout, o cliente é derrubado da lista dos hosts, o endereço IP liberado e a sessão contabilizada a menos desse valor.

- Keepalive Timeout (time | none; default: 00:02:00)

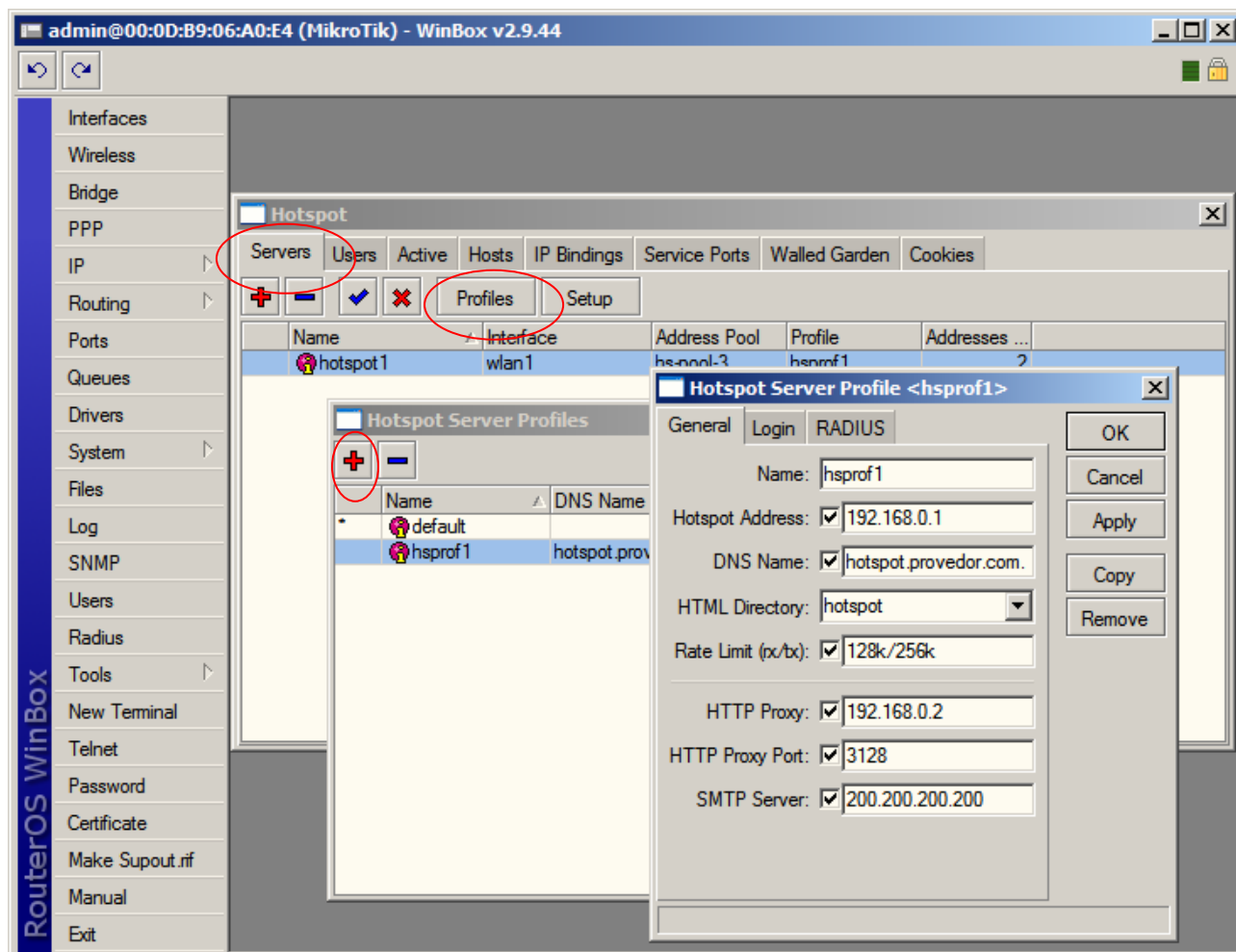
Utilizado para detectar se o computador do cliente está ativo e encontrável. Caso nesse período de tempo o teste falhe, o usuário é tirado da tabela de hosts e o endereço IP que ele estava usando é liberado. O tempo é contabilizado levando em consideração o momento da desconexão menos o valor configurado (2 minutos por default).

- Address Per MAC (integer | unlimited; default 2)

Número de IPs permitidos para um particular MAC.



HOTSPOT SERVER PROFILES



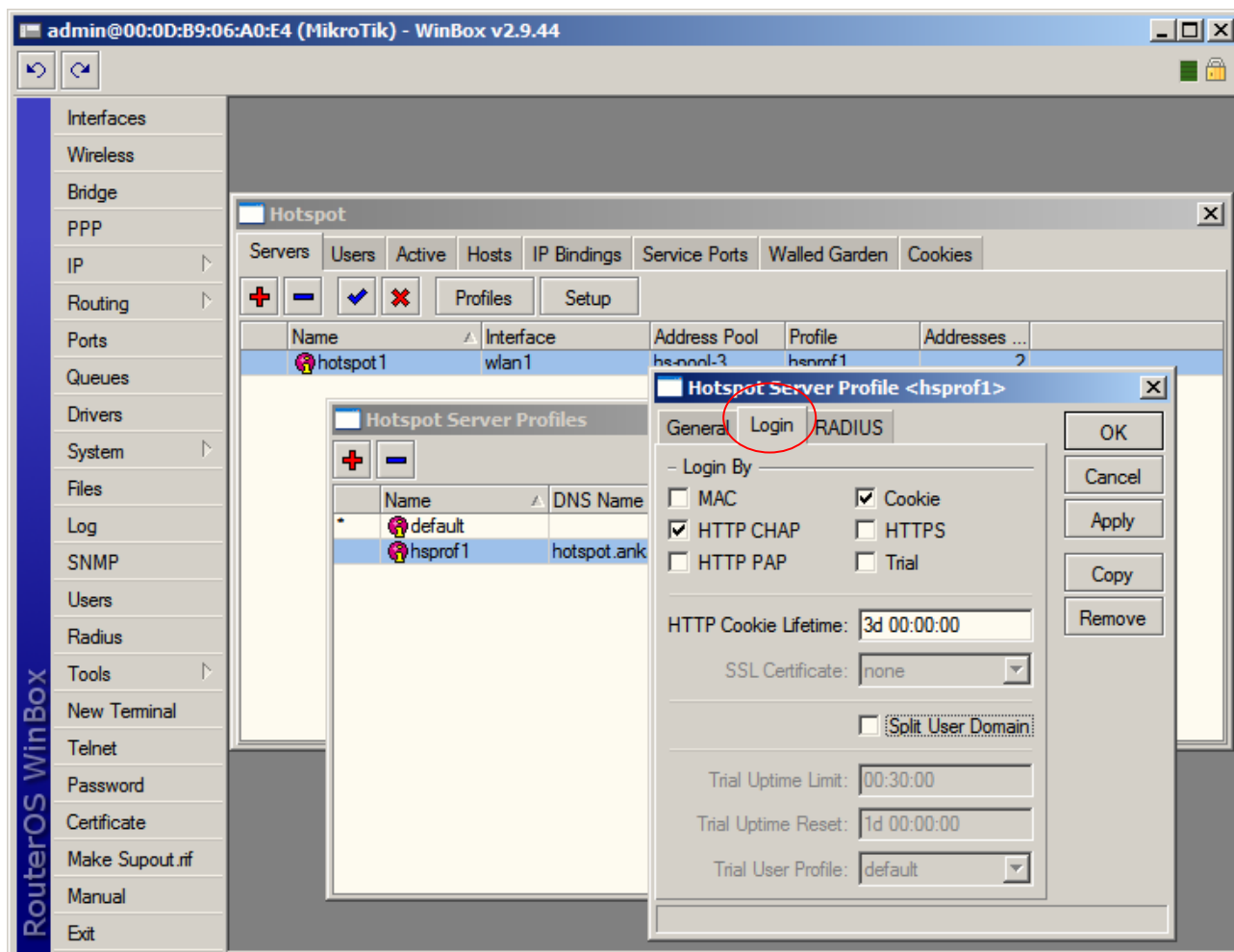
- Rate Limit (rx/tx): (text; default: "")

A limitação de velocidade tem a sintaxe:

rx-rate[/tx-rate][rx-burst-rate[/tx-burst-rate][rx-burst-threshold[/tx-burst-threshold][rx-burst-time[/tx-burst-time]]]]

onde:

- rx é o upload do cliente e tx é o download do cliente;
- as velocidades podem ser números com opcionais "k" (1.000s) e M para kiloo e Mega;
- se tx-rate não é especificado, tem o mesmo valor de rx-rate;
- o mesmo para tx-burst-rate, tx-burst-threshold e tx-burst-time;
- se ambos rx-burst-threshold e tx-burst-threshold não são especificados (mas burst-rate sim), rx-rate e tx-rate são usados como burst threshold;
- se ambos rx-burst-time e tx-burst-time não são especificados, 1s é usado como default.



Login By

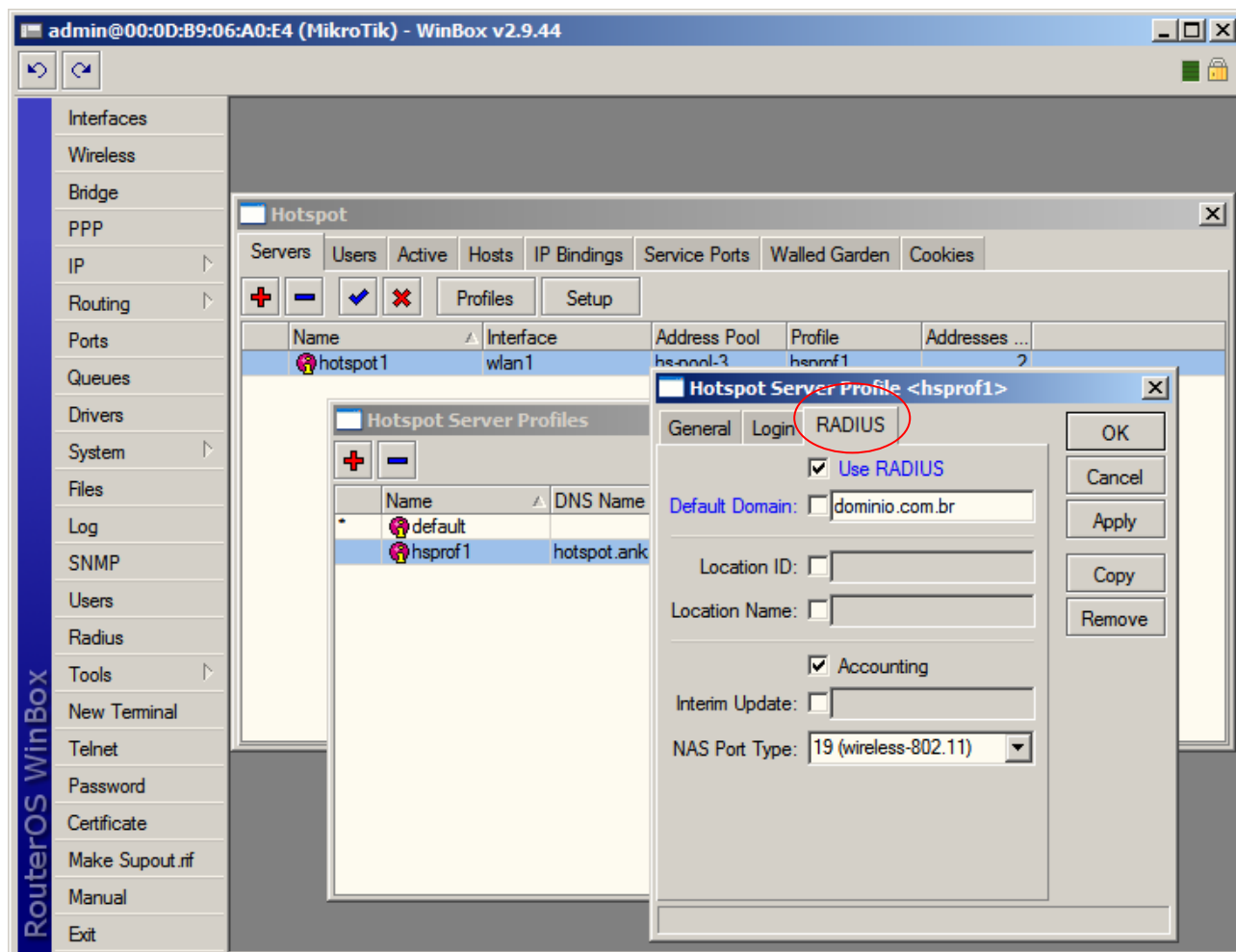
- **MAC** - Tenta usar o MAC dos clientes primeiro como nome de usuário. Se existir na tabela de usuários local ou em um Radius, o cliente é liberado sem login/senha;
- **HTTP CHAP** - Usa método CHAP – Método criptografado;
- **HTTP PAP** - Usa autenticação como texto plano – pode ser sniffado facilmente;
- **Cookie** - Usa http cookies para autenticar sem pedir as credenciais. Se o cliente ainda não tiver um cookie ou tiver expirado, usa outro método;
- **HTTPS** - Usa túnel SSL criptografado. Para isso funcionar, um certificado válido deve ser importado para o roteador.
- **Trial** - Não requer autenticação por um certo período de tempo.

HTTP Cookie Lifetime: tempo de vida dos Cookies

Split User Domain: corta o domínio do usuário no caso de usuário@dominio.com.br



Utilização de Servidor Radius para autenticação do Hotspot



- Location ID

Pode ser atribuído aqui ou no servidor Radius – Normalmente deixar em branco

- Location Name

Pode ser atribuído aqui ou no servidor Radius – Normalmente deixar em branco

- Accounting

Se habilitado, faz a bilhetagem dos usuários, com histórico de logins, desconexões, etc.

- Interim Update

Frequência de envio de informações de accounting (segundos)

0 – assim que ocorre o evento

(Gera tráfego – Interessante que coloque 30 ou 60s)

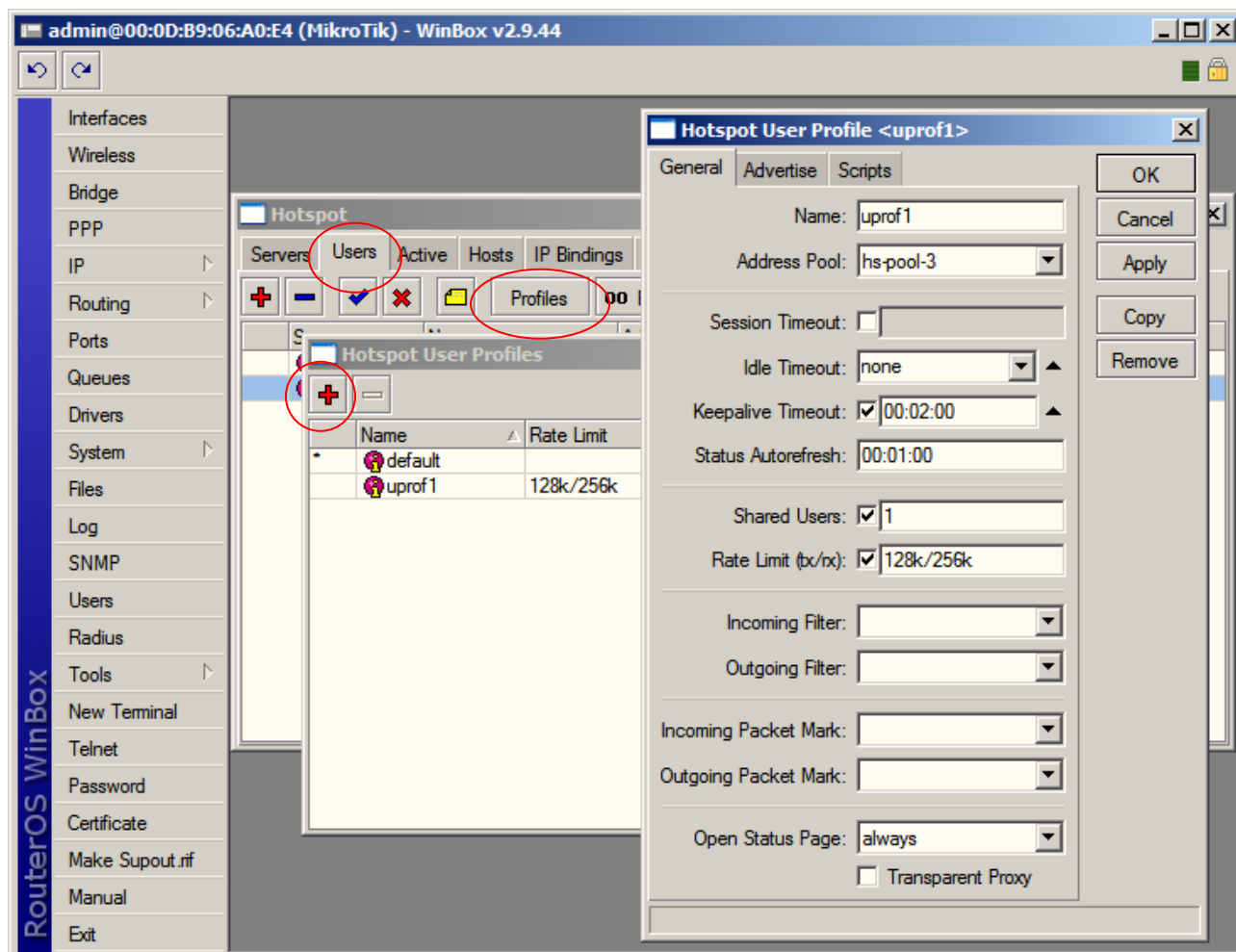
- NAS Port Type

Wireless, Ethernet ou Cabo



HOTSPOT USER PROFILES

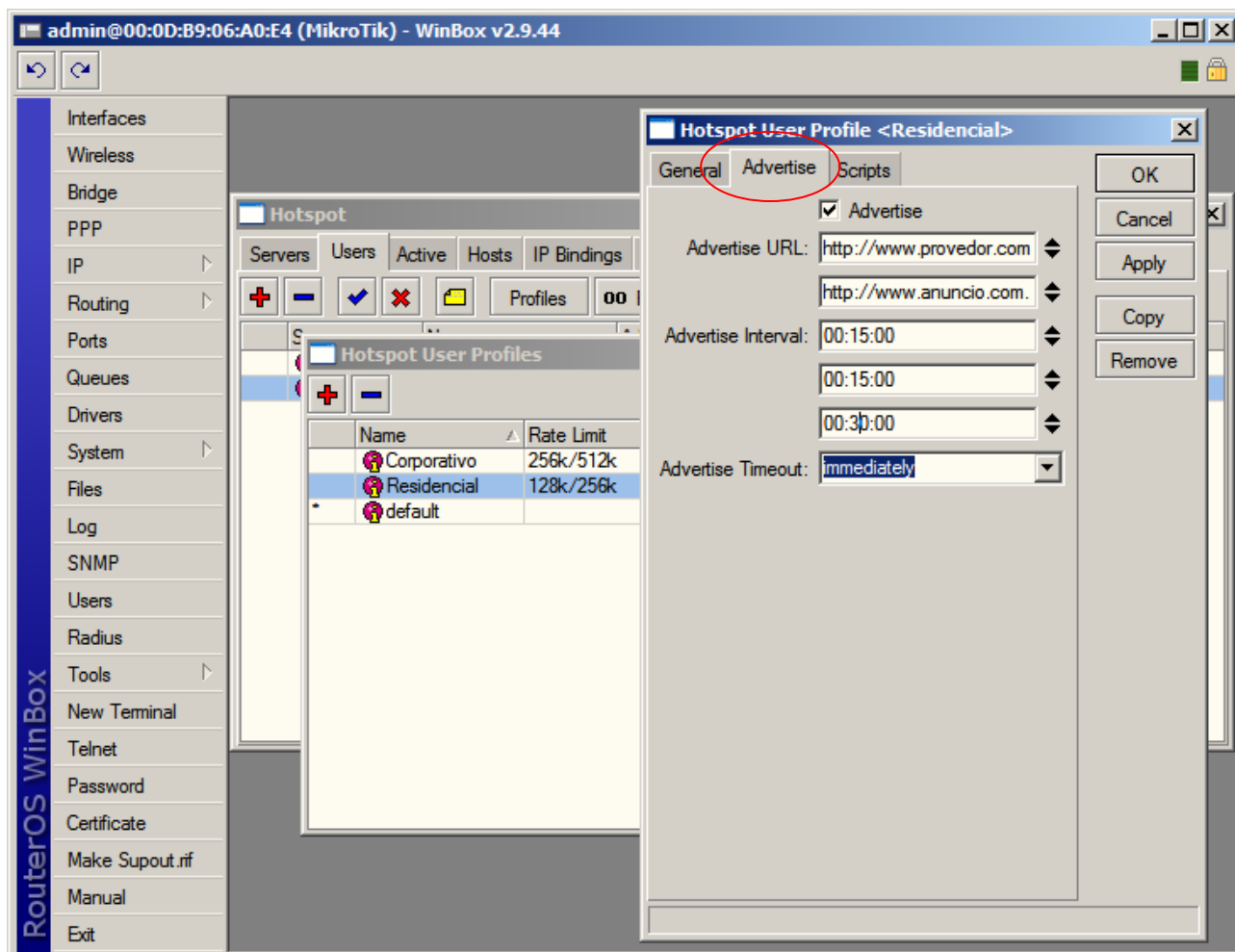
O user profiles servem para dar tratamento diferenciado a grupos de usuários, como, por exemplo, usuários corporativos, usuários residenciais, etc.



- **Session Timeout:** Tempo máximo permitido (depois disso o cliente é derrubado)
- **Idle timeout:** período de inatividade (acesso externo)
- **Keepalive Timeout:** se o computador está “vivo” e tem conectividade
- **Status Autorefresh:** tempo de refresh da página de Status do Hotspot
- **Shared Users:** número máximo permitido de clientes com o mesmo username
- **Rate Limit (tx / rx):** A limitação de velocidade tem a sintaxe:
`rx-rate[/tx-rate][rx-burst-rate[/tx-burst-rate][rx-burst-threshold[/tx-burst-threshold][rx-burst-time[/tx-burst-time]]]]`
 onde:
 - rx e o upload do cliente e tx é o download do cliente;
 - as velocidades podem ser números com opcionais “k” (1.000s) e M para kiloo e Mega;
 - se tx-rate não é especificado, tem o mesmo valor de rx-rate;
 - o mesmo para tx-burst-rate, tx-burst-threshold e tx-burst-time;
 - se ambos rx-burst-threshold e tx-burst-threshold não são especificados (mas burst-rate sim), rx-rate e tx-rate são usados como burst threshold;
 - se ambos rx-burst-time e tx-burst-time não são especificados, 1s é usado como default.



Com a opção Advertise é possível enviar, de tempos em tempos, pop-ups para os usuários do Hotspot



- Advertise URL

Lista das páginas que serão anunciadas. A lista é cíclica, ou seja, quando a última é mostrada, começa-se novamente pela primeira.

- Advertise Interval

Intervalos de exibição dos pop-ups. Depois da sequência terminada, usa sempre o último intervalo. No exemplo, são mostradas a cada 15 minutos, 2 vezes e depois a cada 30 minutos

- Advertise Timeout

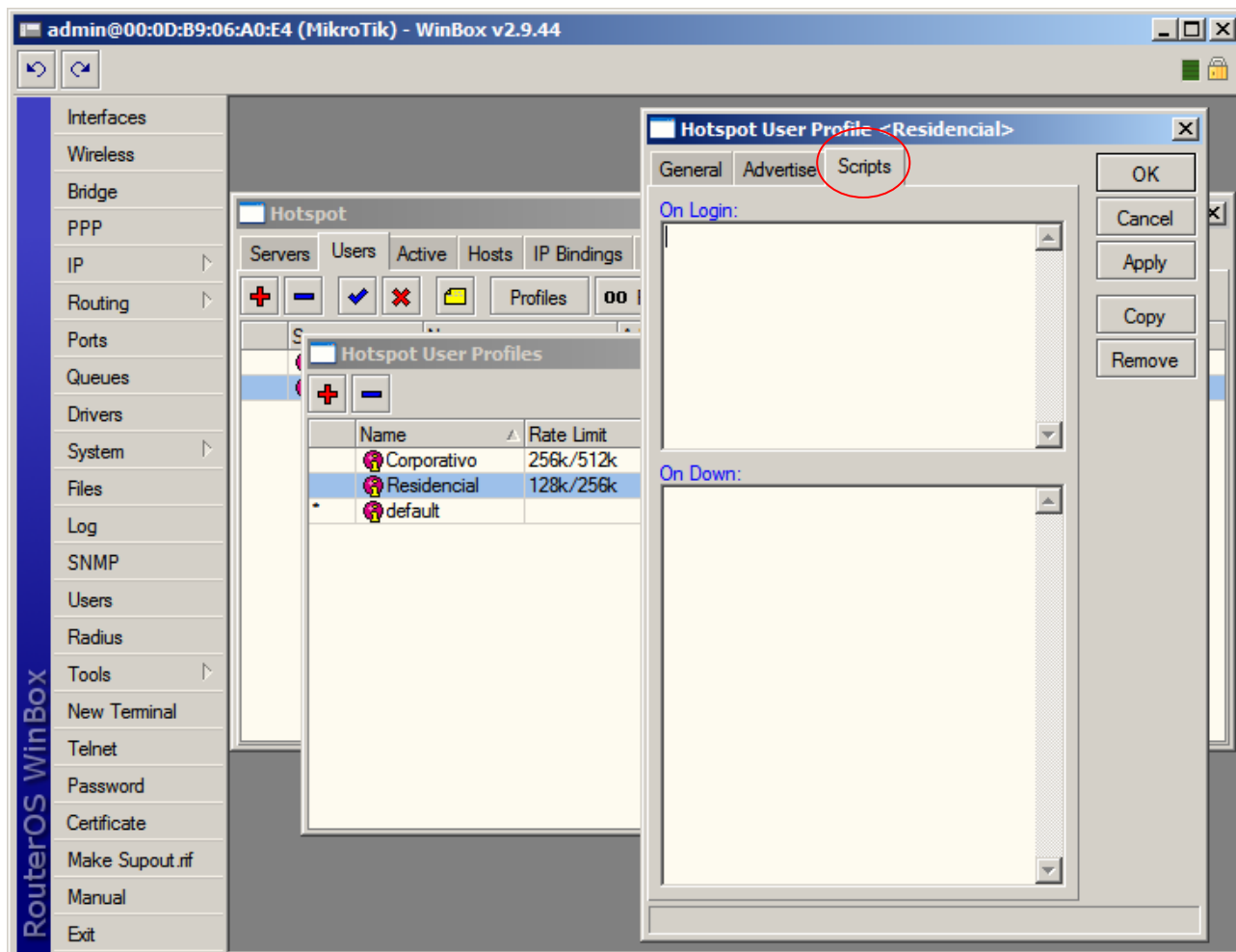
Quanto tempo deve esperar para o anúncio ser mostrado, antes de bloquear o acesso à rede com o "Walled-Garden"

- pode ser configurado um tempo (default = 1 minuto)
- nunca bloquear
- bloquear imediatamente



O Mikrotik possui uma linguagem interna de scripts que podem ser adicionados para serem executados em alguma situação específica

No hotspot é possível criar scripts que executem comandos a medida que um usuário desse perfil se conecta ou se desconecta do Hotspot



Os parâmetros que controlam essas execuções, são:

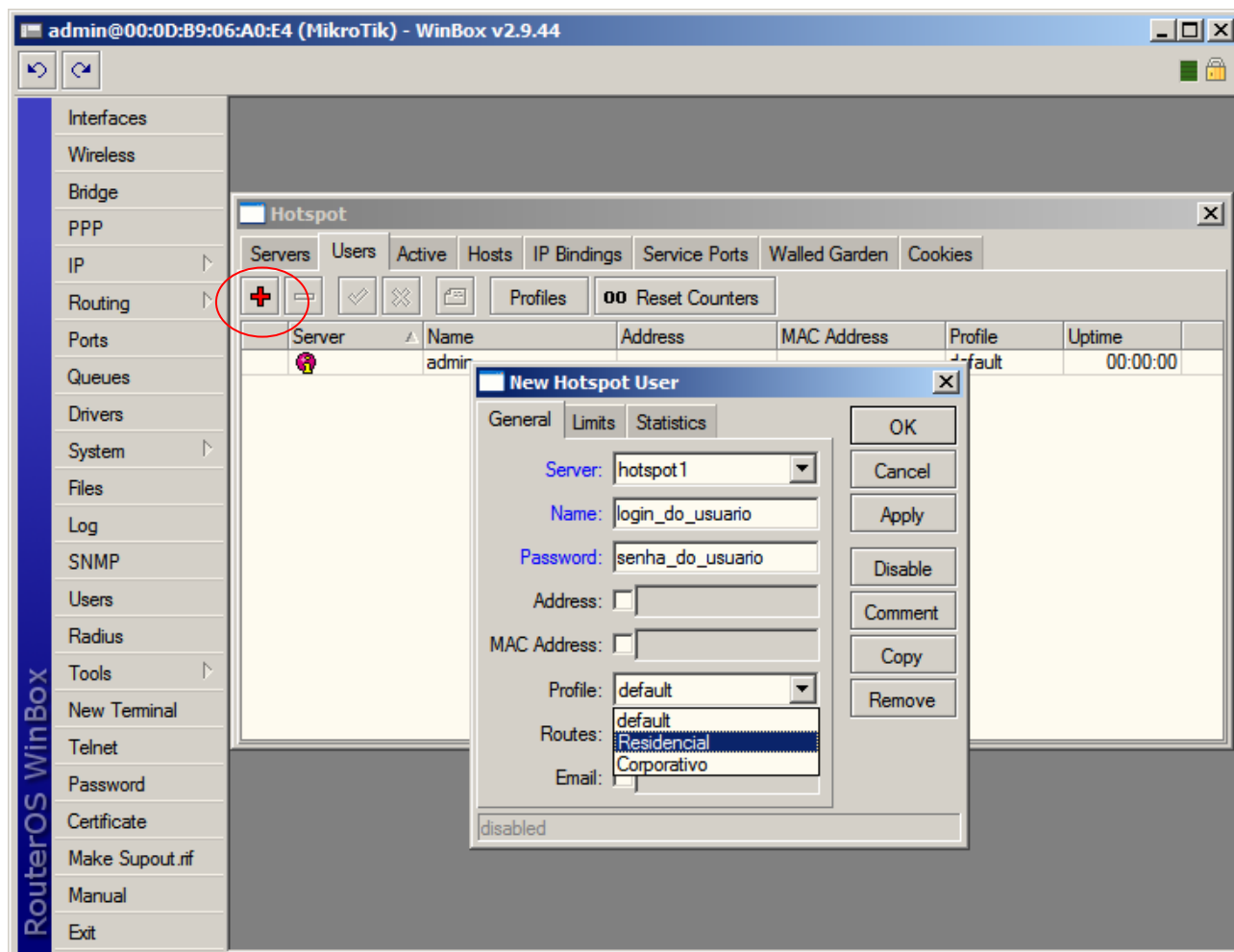
- on-login
- on-logout

Os Scripts são adicionados em Menu System / Scripts



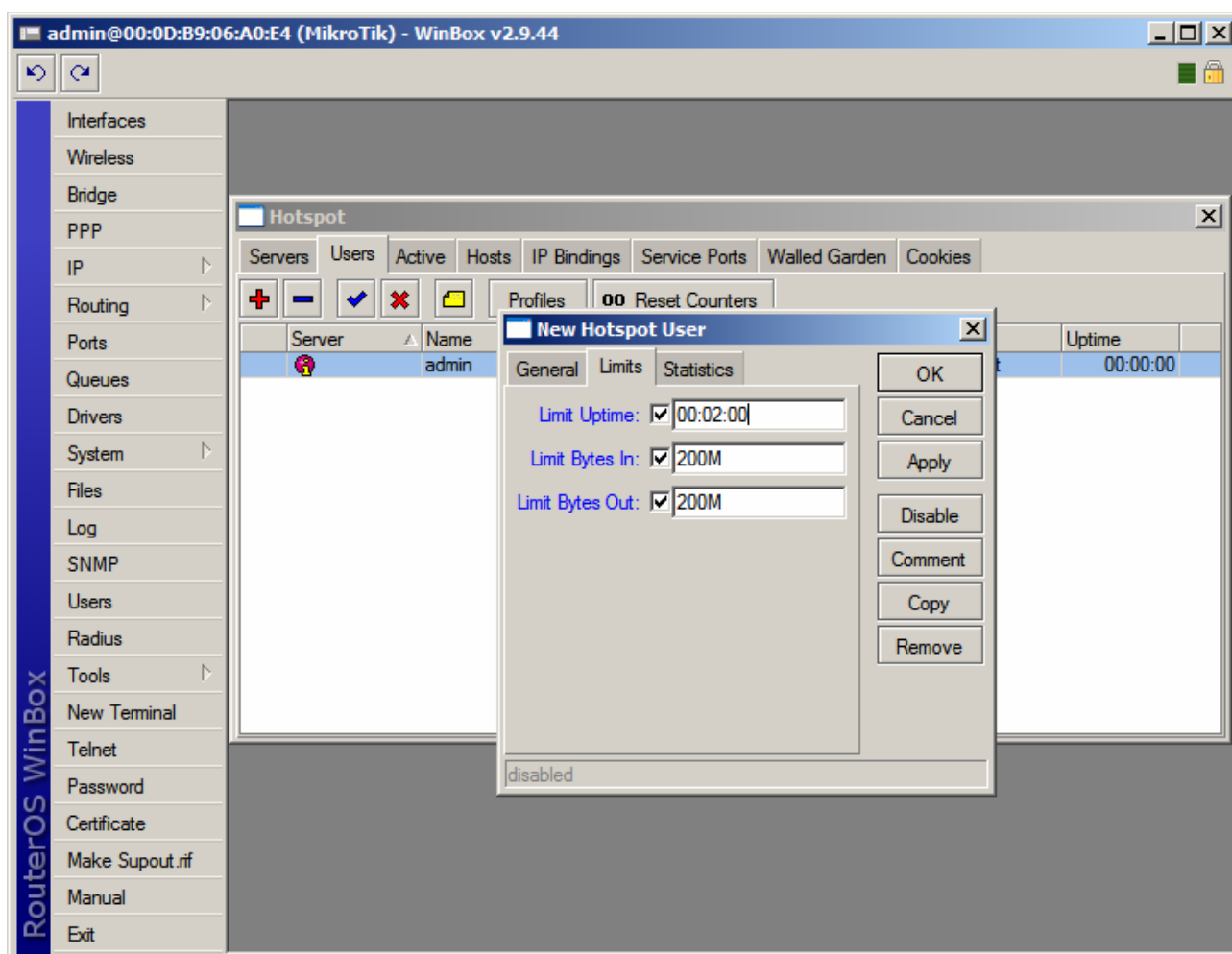
Devemos, agora, cadastrar os usuários que terão permissão para se conectar ao Hotspot.

- Em Hotspot, clique na guia "Users"
- Clique em "Adicionar"
- Clique na guia General
 - Campo Server: "all" para todos os hotspots configurados ou para um específico.
 - Campo Name: Nome do usuário (login). No caso de autenticação por MAC, o MAC pode ser adicionado como username (sem senha)
 - Campo Password: para digitar a senha
 - Campo Address: Caso queira vincular esse usuário a um endereço fixo
 - Campo MAC Address: caso queira vincular esse usuário a um MAC determinado
 - Campo Profile: Perfil de onde esse usuário herda as propriedades
 - Campo Routes: Rota que será adicionada ao cliente quando esse se conectar. Sintaxe de destino gateway métrica. Várias rotas podem ser adicionadas separadas por vírgula.





- Clique na Guia “limits”
 - Campo “Limit Uptime”: Total de tempo que o usuário pode usar o Hotspot. Útil para fazer acesso pré-pago.
Sintaxe: hh:mm:ss.
Default: 0s – Sem limite
 - Campo “Limit Bytes In”: Total de bytes que o usuário pode **transmitir** (bytes que o roteador recebe para o usuário).
 - Campo “Limit Bytes Out”: Total de bytes que o usuário pode **receber** (bytes que o roteador transmite para o usuário).



Se um usuário tem o endereço IP especificado, somente poderá haver 01 (um) logado. Caso outro entre com o mesmo usuário/senha, o primeiro será desconectado.



WALLED GARDEN (JARDIM MURADO)

Configurando um Walled Garden é possível oferecer ao usuário o acesso a determinados serviços sem necessidade de autenticação.

Exemplo: Em um aeroporto pode-se disponibilizar informações climáticas, horários de vôos, etc, se a necessidade de o usuário adquirir créditos para acesso externo.

Quando um usuário não logado no Hotspot requisita um serviço do Walled Garden, o gateway não o intercepta e, no caso de http, redireciona a requisição para o destino ou para o Proxy.

Para implementar o Walled Garden para requisições http, existe um Web Proxy embarcado no Mikrotik, de forma que todas as requisições de usuários não autorizados passem de fato por esse Proxy.

Observar que o Proxy embarcado não tem as funções de fazer cache, pelo menos por ora. Notar, também, que esse Proxy embarcado faz parte do pacote **system** e não requer o pacote **web-proxy**.

É importante salientar que o Walled Garden não se destina somente a serviços WEB, mas qualquer serviço que queiramos configurar. Para tanto, existem 2 menus distintos que são apresentados abaixo, sendo que o primeiro destina-se somente para HTTP e HTTPS e o da segundo para os outros serviços e protocolos.

Walled Garden para http e HTTPS

Action: allow ou deny – permite ou nega

- Server: Hotspot ou Hotspots para o qual vale esse Walled Garden
- Src Address: endereço IP do usuário requisitante
- Dst Address: endereço IP do Web Server
- Method: método de http
- Dst Host: nome de domínio do servidor de destino
- Dst Port: porta de destino que o cliente manda a solicitação
- Path: caminho da requisição

Observação:



- nos nomes de domínio, é necessário o nome completo, podendo ser usado coringas
- aceita-se expressões regulares devendo ser iniciadas com dois pontos (:)



Walled Garden para outros protocolos

Action: aceita, descarta ou rejeita o pacote

- Server: Hotspot ou Hotspots para o qual vale esse Walled Garden
- Src Address: endereço IP de origem do usuário requisitante
- Protocol: Protocolo a ser escolhido da lista
- Dst Port: Porta TCP ou UDP que está sendo requisitado
- Dst Host: Nome de domínio do WEB Server

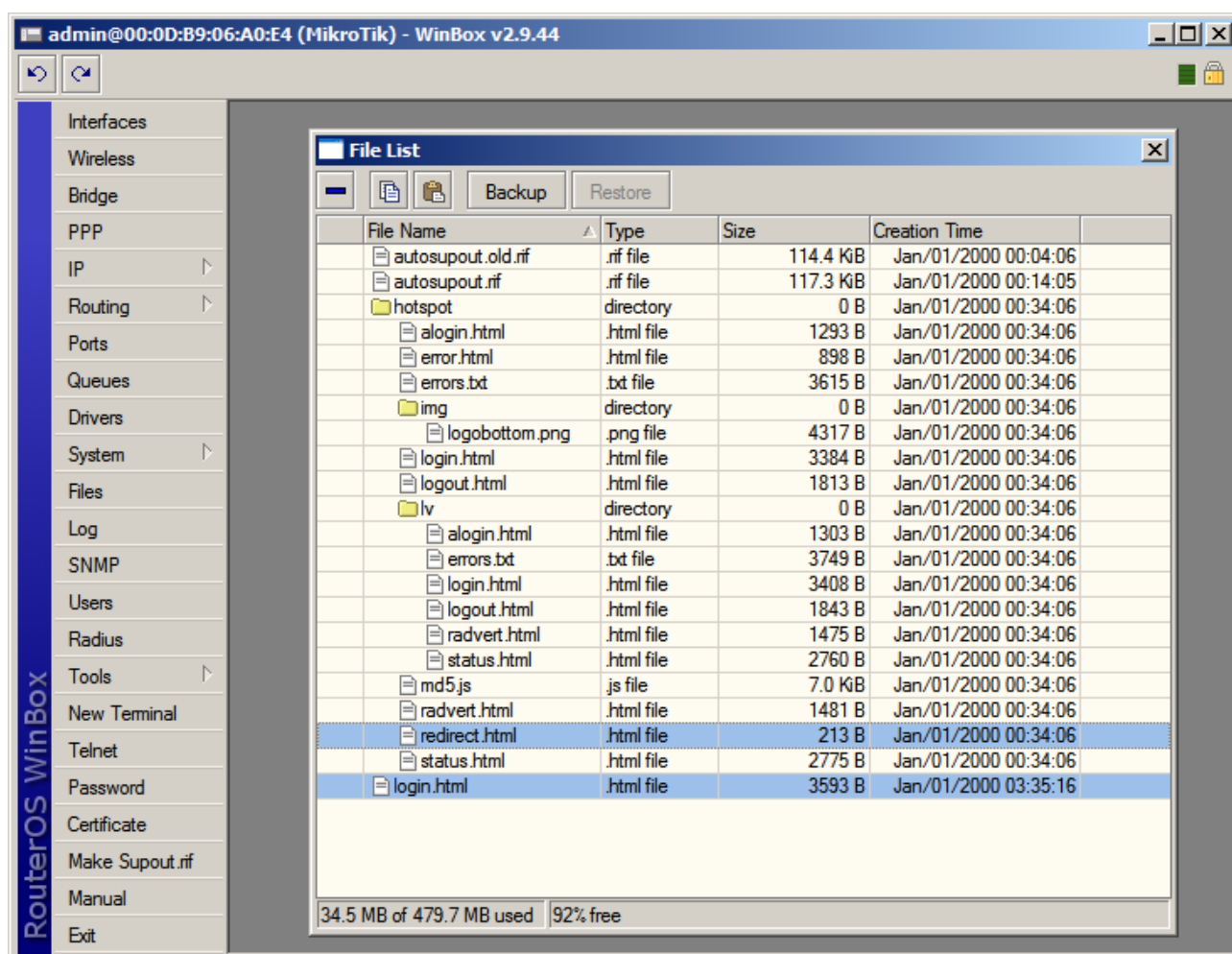


PERSONALIZANDO O HOTSPOT

As páginas do Hotspot são totalmente configuráveis e podem ser editadas em qualquer editor HTML, sendo posteriormente atualizadas no Mikrotik.

Além disso, é possível criar conjuntos totalmente diferentes das páginas do Hotspot para vários perfis de usuários especificando diferentes diretórios html raiz na opção html-directory em Hotspot Profile.

Essa possibilidade, associada a criação de Aps virtuais possibilita que, em uma mesma área pública o detentor de infra-estrutura possa, de forma transparente, servir a vários operadores, utilizando os mesmos equipamentos.



Principais páginas HTML que são mostradas aos usuários:

- redirect.html – redireciona o usuário para outra URL (exemplo: a página de login)
- login.html - Página de login mostrada a um usuário solicitando nome e senha. Esta página pode ter os seguintes parâmetros:
 - username – nome do usuários
 - password – senha
 - dst – URL original requisitada antes de cair na tela de login. O usuário será enviado a esta URL após um login bem-sucedido
 - pop-up – se deve ser aberta uma janela de pop-up após o login

REDIRECIONANDO TRÁFEGO DE SMTP PARA SEU DEVIDO SERVIDOR



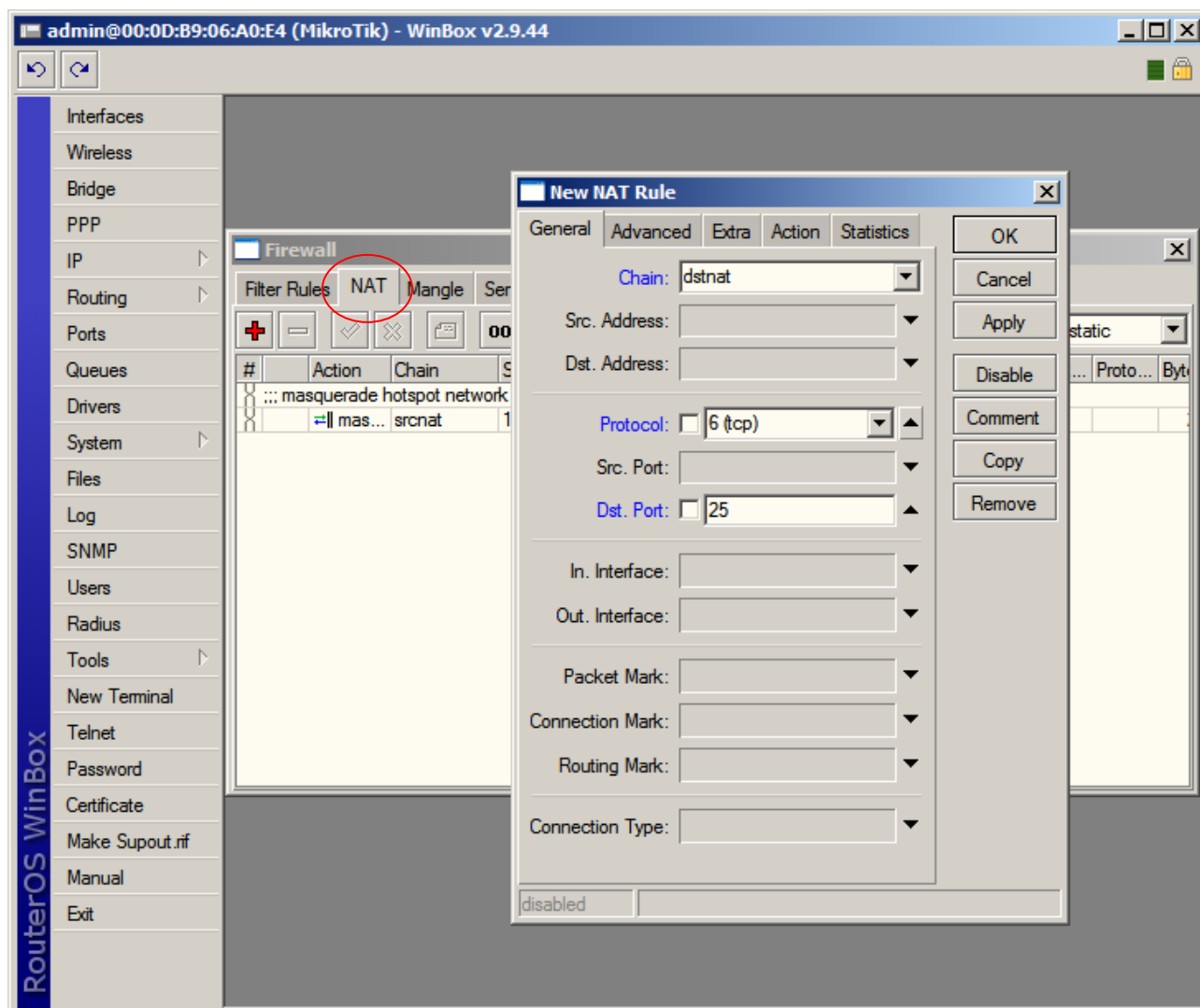
Você pode redirecionar todo o tráfego através de seu Router para o seu próprio Servidor de E-mail.

- Clique no Menu "IP"
- Clique na opção "Firewall"



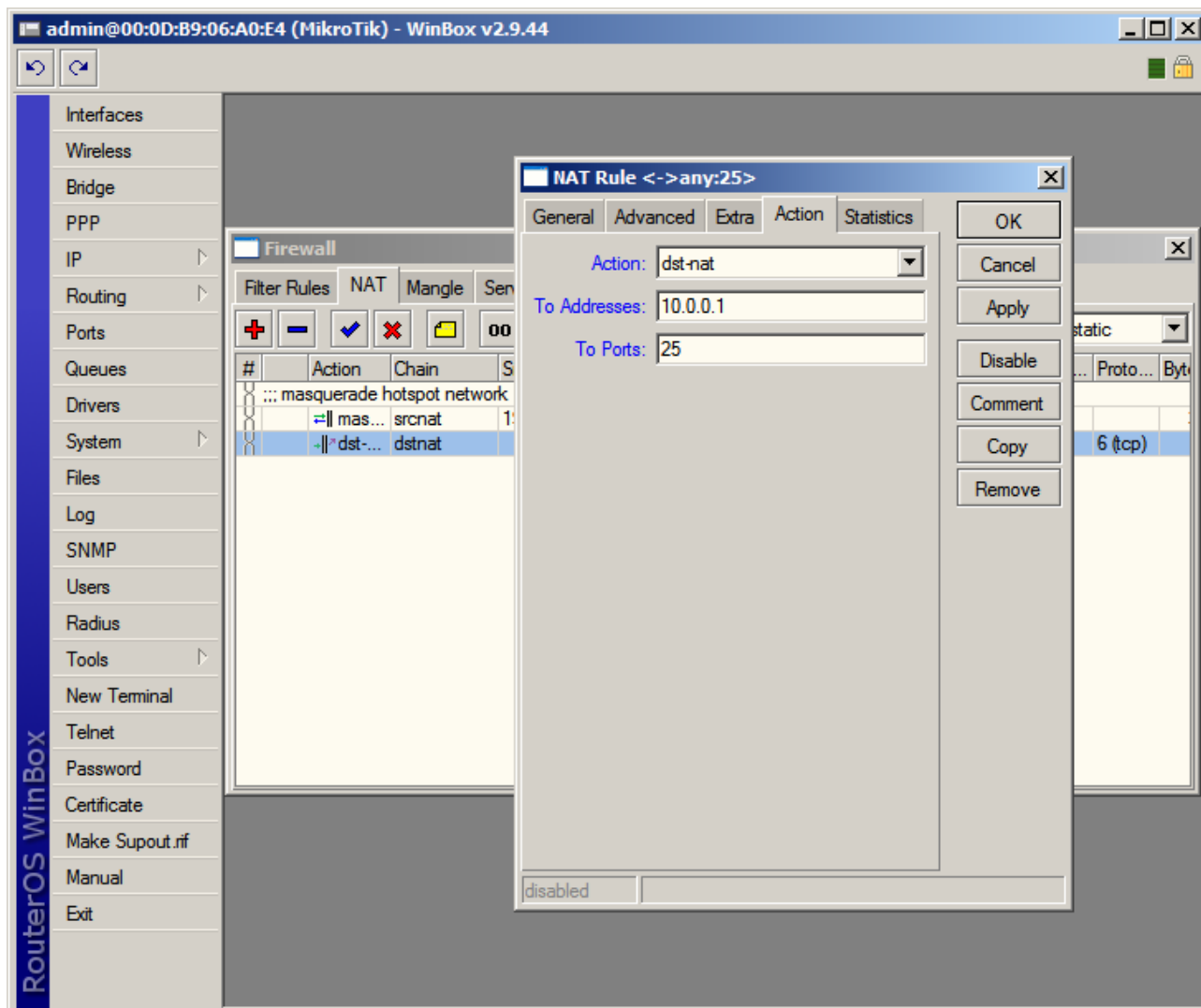


- Clique na guia “NAT”
- Clique em “Adicionar”
- Na guia “General”, na opção “Chain”, escolha a opção “dstnat”
- Na opção “Protocol”, escolha “TCP”
- Na opção “Dst. Port.”, escolha a porta 25





- Clique na guia "Action"
- Na opção "Action", escolha a opção "dst-nat"
- Na opção "To Addresses", digite o IP do servidor de email
- Na opção "To Ports", digite a porta SMTP, 25.
- Clique no botão "OK"





Referências:

- Mikrotik Wiki - <http://wiki.mikrotik.com/wiki/>
- Apostila Curso Router-OS Mikrotik – Wlan Brasil
- Certificado SSL - <http://www.laniway.com.br>

Cópia autorizada: Marcelo Carvalho - MACNet (AWS)