

MPLS

PPP

wireless

firewall

QoS



md brasil

Servidor de autenticação usando **MetaRouter** e **OpenWRT**

MUM Brasil – Rio de Janeiro – Novembro/2009

Sérgio Souza

MPLS

PPP

wireless

firewall

QoS



Nome: Sergio Souza

- ◆ Tecnólogo em Processamento de Dados
- ◆ Consultor independente atuando há vários anos em implementação, manutenção e gerenciamento de redes estruturadas e redes sem fio
- ◆ Consultor em implementação e manutenção de sistemas livres baseados em GNU/Linux
- ◆ Administrador do provedor de serviços gerenciados **Via Livre**
- ◆ Instrutor Mikrotik Brasil
- ◆ Parceiro MD Brasil em soluções de TI e Consultoria

MPLS

PPP

wireless

firewall

QoS



Objetivos

- ◆ O objetivo é apresentar uma solução baseada em virtualização do sistema operacional GNU/Linux OpenWRT, através do MetaRouter, ferramenta de virtualização do Mikrotik ROS.
- ◆ Será demonstrado um servidor Freeradius e servidor web provendo uma página de cadastro para clientes e a inserção dos dados no arquivo users do Freeradius.
- ◆ Serão abordados os passos de instalação das ferramentas.

MPLS

PPP

wireless

firewall

QoS

enlaces



md brasil

Vantagens da Virtualização

- ◆ Gerenciamento centralizado
- ◆ Instalações simplificadas
- ◆ Facilidade para a execução de backups
- ◆ Suporte e manutenção simplificados
- ◆ Acesso controlado a dados privados e à propriedade intelectual, mantendo-os seguros dentro do *data center* da empresa

MPLS

PPP

wireless

firewall

QoS



Vantagens da Virtualização

- ◆ Independência de Hardware
- ◆ Disponibilização de novos ambientes operacionais em poucos minutos
- ◆ Migração de sistemas operacionais para novo hardware de forma transparente
- ◆ Maior disponibilidade e recuperação de sistemas
- ◆ Compatibilidade total com as aplicações

MPLS

PPP

wireless

firewall

QoS



Requisitos

- ◆ 16 MB RAM para cada instância Metarouter, quando virtualizando o Mikrotik ROS.
- ◆ Versão 3.28 ou superior do Mikrotik ROS
- ◆ Qualquer dispositivo RouterBoard da série 400 ou série 1000

MPLS

PPP

wireless

firewall

QoS



Limitações

- ◆ 8 máquinas virtuais (este número aumentará no futuro)
- ◆ 8 interfaces virtuais (caso necessite de mais interfaces deverá lançar mão de recursos VLAN)
- ◆ Não é possível adicionar unidades de armazenamento externas (store) para as máquinas virtuais
- ◆ Limitação de 256 MB RAM (RB450G)

MPLS

PPP

wireless

firewall

QoS



md brasil

Exemplos de utilização

Disponibilizar uma máquina virtual para clientes, onde os mesmos possam personalizar seu ambiente.

Exemplo:

Um Provedor poderá criar um roteador virtual em uma porta ethernet, onde o cliente personalizará seu firewall e limitação de banda, deixando as configurações do roteador principal, inalteradas.

MPLS

PPP

wireless

firewall

QoS

enlaces



md brasil

OpenWrt
Wireless Freedom

É um firmware para roteadores com Linux embarcado. Trata-se de uma mini-distribuição desenvolvida sob a GPL (General Public License). Mini-distribuição porque o número de funções é reduzido perante distribuições completas como: SuSe, Mandriva, Slackware, entre outros. Isto ocorre devido a limitação das memórias dos roteadores, consideravelmente menores comparadas a computadores pessoais comuns, pois raramente possuem mais do que 32MB de RAM e 8MB de ROM.

MPLS

PPP

wireless

firewall

QoS

enlaces



md brasil

OpenWrt
Wireless Freedom

Apesar do número de funções reduzido, podemos personalizá-lo e usufruir de várias serviços, como servidor web Apache ou Lighttpd, PHP, Freeradius, entre outros.

O sistema é altamente personalizável.

MPLS

PPP

wireless

firewall

QoS



Instalação

Para a instalação de uma imagem do OpenWRT, previamente compilada, basta realizar o download no link abaixo:

<http://www.mikrotik.com/download/openwrt-metarouter-rootfs-1.1.tgz>

Após o download enviar (upload) o arquivo para o menu FILES do Mikrotik ROS e seguir as instruções abaixo

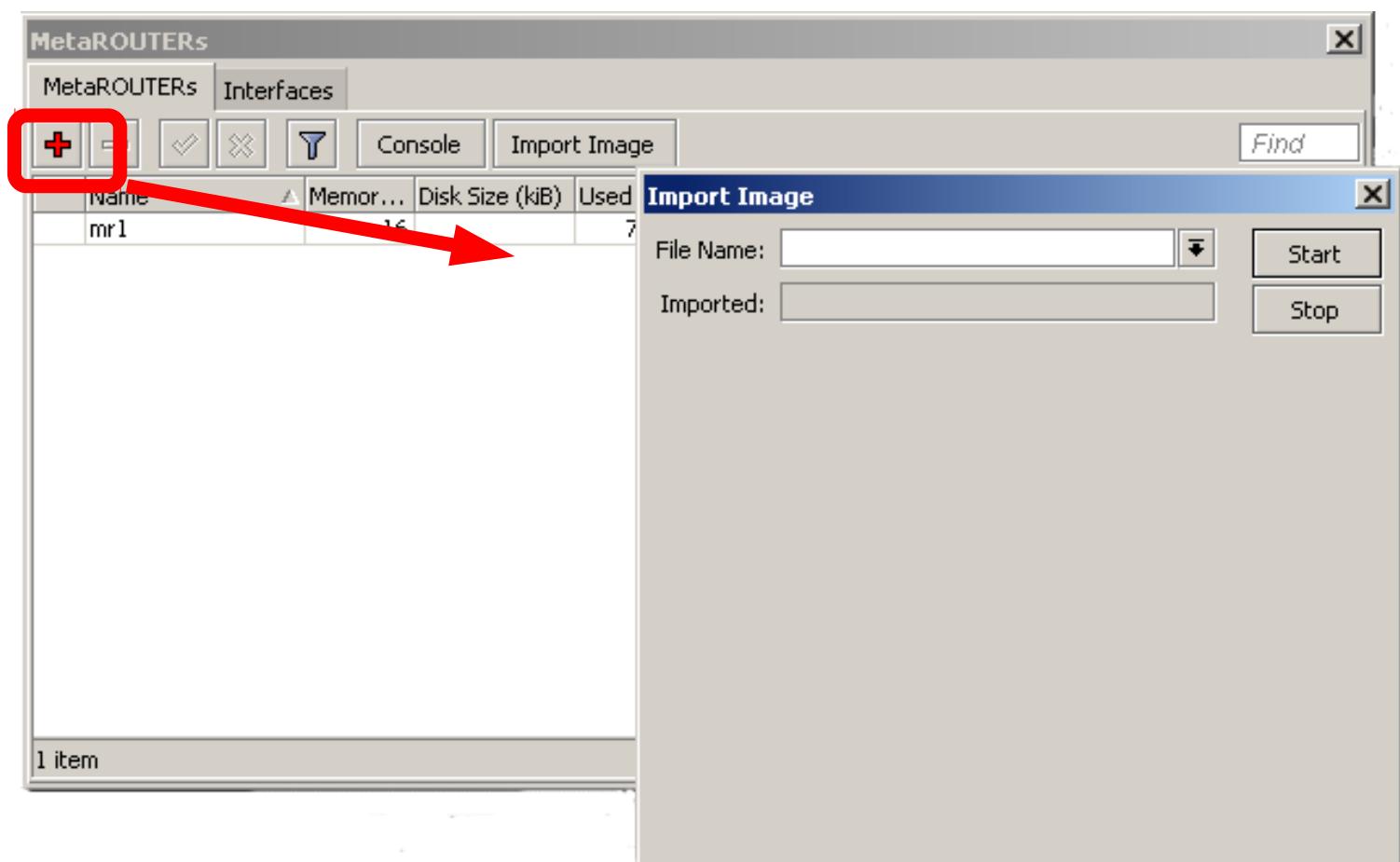
MPLS
PPP

QoS

Instalação



md brasil



MPLS
PPP

QoS

VPN
OpenS
firewall

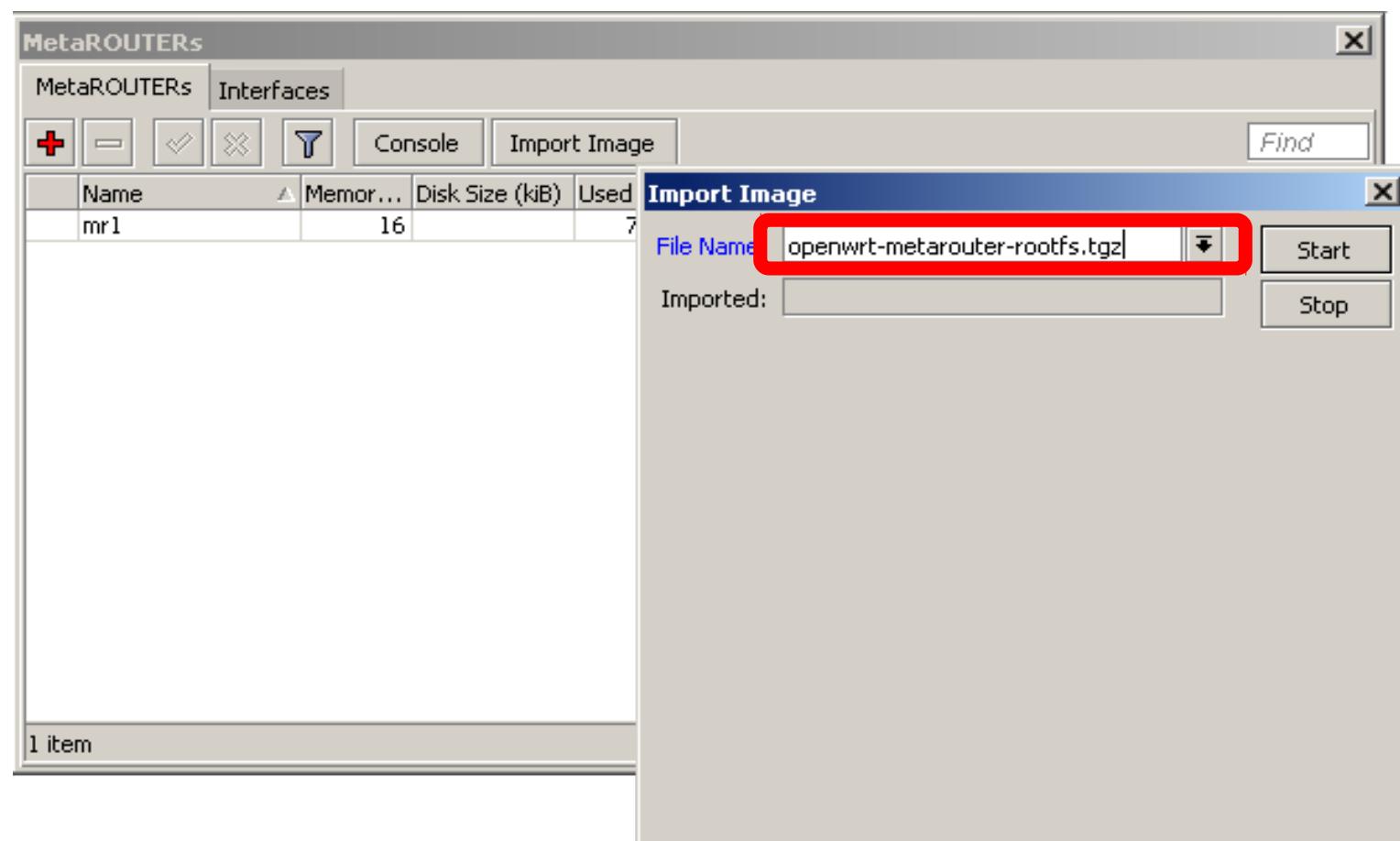
wireless

enlaces



md brasil

Instalação



MPLS
PPP

QoS

Instalação



md brasil

MetaROUTERS

MetaROUTERS Interfaces

Console Import Image Find

Name	Memory	Disk Size (kB)	Used D	Status
mr1	16	7600		running

MetaROUTERS Interfaces

Find

Virtual Machine	Type	Static Interface	VM MAC Address
mr1	dynamic		02:BF:76:FB:4E:7A

VM Interface <02:BF:76:FB:4E:7A>

Virtual Machine: mr1 OK Cancel

Type: dynamic static Apply

Dynamic MAC Address: 02:99:A4:DC:F0:B1 Disable

Dynamic Bridge: none Copy

VM MAC Address: 02:BF:76:FB:4E:7A Remove

disabled

1 item (1 selected)

MPLS

PPP

wireless

firewall

QoS



Instalação

Como pudemos observar a criação de uma máquina virtual é bastante simples; é necessário apenas especificar o nome da mesma e quantidade de RAM dispensada. O tamanho do disco poderá ser configurado para dinâmico ou um valor fixo.

Observação

Quando deixar configurado o tamanho do disco para dinâmico, se possuir uma aplicação que gere muitos dados, o mesmo poderá encher rapidamente acarretando problemas para a máquina virtual e para o host anfitrião (máquina principal).

Caso seja adicionada uma nova máquina virtual, sem especificar nenhum parâmetro, ela será criada com tamanho do disco dinâmico e 16 MiB de RAM.

MPLS

PPP

wireless

firewall

QoS



Instalação

Caso tenha interesse poderá realizar uma compilação do OpenWRT e personalizá-lo de acordo com suas necessidades.

Utilizando um sistema Gnu/Linux qualquer; via SVN baixe o último código fonte disponível

[svn co svn://svn.openwrt.org/openwrt/trunk](http://svn.openwrt.org/openwrt/trunk)

MPLS

PPP

wireless

firewall

QoS



Instalação

Realize o download do patch MetaRouter, conforme abaixo

```
cd trunk/
```

```
wget http://www.mikrotik.com/download/openwrt-metarouter-1.1.patch
```

```
patch -p0 <openwrt-metarouter-1.1.patch
```

MPLS
PPP

QoS
firewall
enlaces

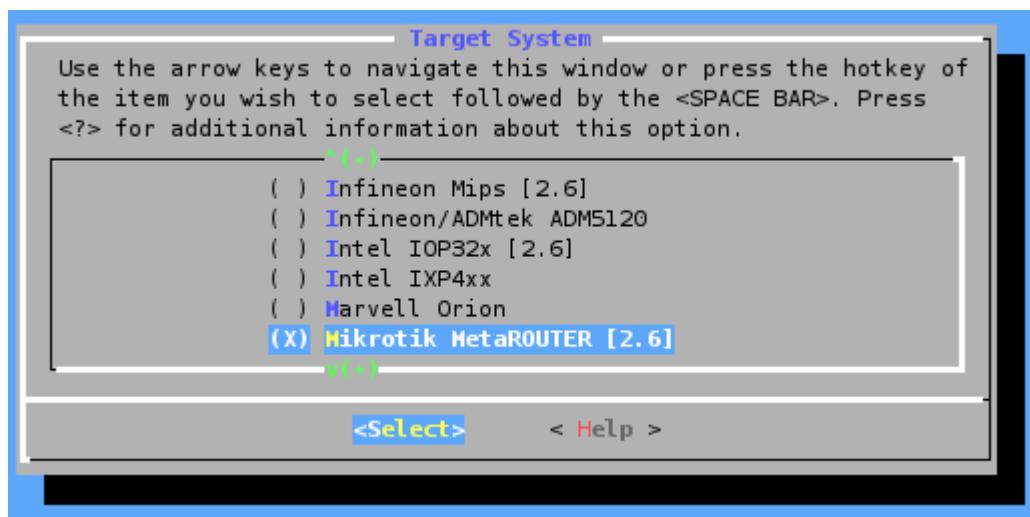


md brasil

Instalação

Após aplicar o patch, execute:

make menuconfig



Acesse o menu Target System e escolha Mikrotik MetaRouter

Poderá adicionar suporte a outras funções, basta seleciona-las nos menus apropriados.

Após definir todas as funções, encerre o menu.

Caso possua qualquer erro ou dependência o sistema exibirá um alerta.
Deverá corrigi-los antes de prosseguir.

Execute, em seguida:

make

Quando terminar a compilação, terá uma imagem no formato tgz para importar.

MPLS

PPP

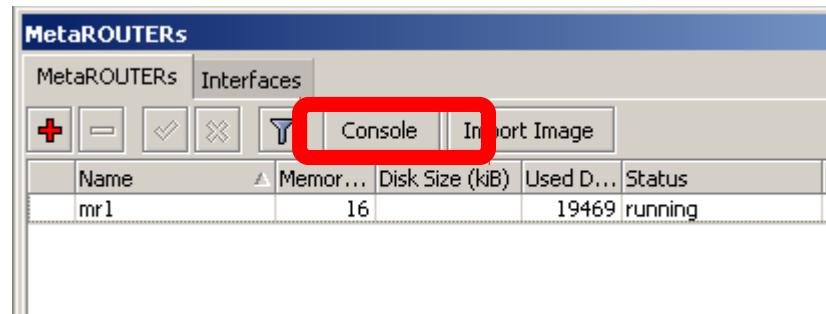
QoS

OpenS
firewall

wireless



Após a instalação do OpenWRT podemos acessá-lo via console e configurar o endereço IP para acessarmos remotamente.



```
uci set network.lan.ipaddr=172.31.1.249
uci set network.lan.netmask=255.255.255.248
uci set network.lan.gateway=172.31.1.254
uci set network.lan.dns=208.67.222.222
uci set system.@system[0].hostname=MDBrOpenWRT
uci commit
/etc/init.d/dnsmasq stop
/etc/init.d/dnsmasq disable
reboot
```

MPLS

PPP

wireless

firewall

QoS



Poderemos agora instalar pacotes de software adicionais que compilamos ou podemos instalar pacotes previamente compilados, desde que sejam compatíveis com a imagem instalada.

O endereço de um sítio da Internet que podemos encontrar uma imagem do OpenWRT compilada, assim como vários pacotes de softwares encontra-se abaixo:

<http://openwrt.pantele.com.ua/trunk/metarouter/>

<http://openwrt.pantele.com.ua/trunk/metarouter/packages/>

MPLS

PPP

wireless

firewall

QoS



Exemplo de instalação de um pacote

Acesse o OpenWRT

```
cd /tmp
```

```
wget http://openwrt.pantele.com.ua/trunk/metarouter/packages/freeradius2_2.1.4-1_metarouter.ipk
```

```
opkg install freeradius2_2.1.4-1_metarouter.ipk
```

Caso seja exibido alguma dependência de aplicação, realize o download da mesma e instale previamente. Realize o procedimento de instalação do pacote novamente.

MPLS

PPP

wireless

firewall

QoS



Os pacotes utilizados nesta configuração, além dos pacotes já disponíveis na própria imagem, foram:

cgilib - 0.7-1
freeradius2 - 2.1.4-1
libgd - 2.0.35-1
libiconv - 1.11-1
libiptc - 1.4.4-2
libjpeg - 6b-1
libltdl - 1.5.26-1
libpcre - 7.9-1
Libpng - 1.2.40-1
lighttpd - 1.4.23-1
lighttpd-mod-cgi - 1.4.23-1

lighttpd-mod-simple-vhost – 1.4.23-1
lighttpd-mod-status – 1.4.23-1
mini-sendmail - 1.3.6-2
nano - 2.1.11-1
php5 - 5.2.6-3
php5-cgi - 5.2.6-3
php5-fastcgi - 5.2.6-3
php5-mod-gd - 5.2.6-3
zlib - 1.2.3-5



Após a instalação de todos os serviços necessários podemos iniciá-los via init.d

**/etc/init.d/radiusd start
/etc/init.d/lighttpd start**

Para verificarmos os Serviços em execução:

ps ax

PID	USER	VSZ	STAT	COMMAND
1	root	1456	S	init
2	root	0	SW<	[kthreadd]
3	root	0	SW<	[ksoftirqd/0]
4	root	0	SW<	[events/0]
5	root	0	SW<	[khelper]
21	root	0	SW<	[kblockd/0]
41	root	0	SW	[pdflush]
42	root	0	SW	[pdflush]
43	root	0	SW<	[kswapd0]
44	root	0	SW<	[aio/0]
627	root	0	SW<	[khvcd]
1273	root	1456	S	init
1282	root	1460	S	syslogd -C16
1284	root	1440	S	klogd
1296	root	868	S	/sbin/hotplug2 --override --persistent --set-worker /
1628	root	1124	S	/usr/sbin/dropbear -p 22 -P /var/run/dropbear.1.pid
1634	root	3200	S	lighttpd -f /etc/lighttpd/lighttpd.conf
1648	root	1180	R	/usr/sbin/dropbear -p 22 -P /var/run/dropbear.1.pid
1649	root	1464	S	-ash
1692	root	3308	S	radiusd -i 172.31.1.249 -p 1812,1813
1693	root	3308	S	radiusd -i 172.31.1.249 -p 1812,1813
1694	root	3308	S	radiusd -i 172.31.1.249 -p 1812,1813
1695	root	3308	S	radiusd -i 172.31.1.249 -p 1812,1813
1696	root	3308	S	radiusd -i 172.31.1.249 -p 1812,1813
1697	root	3308	S	radiusd -i 172.31.1.249 -p 1812,1813
1698	root	3308	S	radiusd -i 172.31.1.249 -p 1812,1813
1700	root	1440	S	

MPLS

PPP

wireless

firewall

QoS



Em seguida poderemos criar as páginas html/php para inserirmos os dados do cadastro dos clientes com os dados de acesso.

Nesta configuração é usada apenas um exemplo em html/php para escrever em um arquivo texto (users), o qual o Freeradius usará como base de dados.

Podemos utilizar banco de dados como o sqlite ou o mysql para provermos um método mais eficiente de armazenamento.

MPLS

PPP

QoS

Wireless firewalls enlaces



md brasil

Exemplo de um formulário HTML

```
<html>

    <head>
        <meta http-equiv="Content-Language" content="pt-br">
        <meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
        <title>Cadastro Clientes</title>
    </head>

    <body>
        <br><br>
        <p>Cadastro de clientes:</p>

        <form method="post" action="gravar.php">
            <p>Nome: <input type="text" name="txt_nome" size="20"></p>
            <p>Senha: <input type="text" name="txt_senha" size="20"></p>
            <p>Framed-IP: <input type="text" name="txt_ipaddr" size="20"></p>
            <p>Framed-Protocol: <input type="text" name="txt_proto" size="20"></p>
            <p>Framed-MTU: <input type="text" name="txt_mtu" size="20"></p>
            <p><input type="submit" value="Gravar" name="btnOK">
                <input type="reset" value="Zerar campos" name="B2"></p>
        </form>

    </body>

</html>
```

MPLS

PPP

QoS

Wireless firewalls enlaces



PHP para gravar arquivo com as configurações

```
<?php
//PEGA OS DADOS ENVIADOS PELO FORMULARIO
$nome = $_POST["txt_nome"];
$senha = $_POST["txt_senha"];
$ip = $_POST["txt_ipaddr"];
$protocolo = $_POST["txt_proto"];
$valormtu = $_POST["txt_mtu"];

//PREPARA O CONTEUDO A SER GRAVADO
$conteudo =
$nome   Cleartext-Password := '$senha'
        FRAMED-IP-Address = $ip,
        Framed-Protocol = $protocolo,
        Framed-MTU = $valormtu

";

//ARQUIVO TXT
$arquivo = "/etc/freeradius2/users";

//TENTA ABRIR O ARQUIVO
if (!$abrir = fopen($arquivo, "a")) { echo "Erro abrindo arquivo ($arquivo)"; exit; }
//ESCREVE NO ARQUIVO

if (!fwrite($abrir, $conteudo)) { print "Erro escrevendo no arquivo ($arquivo)"; exit; } echo "Cadastro realizado com sucesso!";
;

//FECHA O ARQUIVO fclose($abrir);
?>
```

MPLS

PPP

wireless

firewall

QoS



Com estas simples configurações podemos visualizar N soluções para integração do Mikrotik ROS e sistemas virtualizados.

- ◆ Relay SMTP para o The Dude (mini-sendmail)
- ◆ Servidor HTTP para mensagens aos clientes
- ◆ Asterisk
- ◆ Openser (sip proxy)
- ◆ Base de dados de usuários (freeradius, ldap)

Enfim, qualquer software disponível para o sistema GNU/Linux e compatível com a arquitetura de hardware compilada.

MPLS

PPP

QoS

wireless

firewall

enlaces



Fontes de Referência:

<http://wiki.mikrotik.com/wiki/Metarouter>

<http://forum.mikrotik.com/viewtopic.php?f=15&t=35800>

<http://forum.mikrotik.com/viewtopic.php?f=15&t=32187>

<https://forum.openwrt.org/viewtopic.php?id=10330>

<http://www.rabinovich.org/ymheebcex/>

<http://openwrt.pantele.com.ua/trunk/metarouter/>

<https://forum.openwrt.org/viewtopic.php?id=11301>

<http://nuwiki.openwrt.org/oldwiki/BuildingPackagesHowTo#packagehelloworldpatches100-hello.patch>

MPLS

PPP

wireless

firewall

QoS



md brasil

Obrigado!!

Sergio Souza
Via Livre / MD Brasil
sergio@vialivre.net
sergio@mikrotikbrasil.com.br