

Gerenciando usuários com MikroTik User Manager

Anderson Marin Matozinhos

MTCNA, MTCWE, MTCRE, MTCTCE, MTCINE, MTCUME
MikroTik Official Consultant
MikroTik Certified Training Partner

anderson@icorporation.com.br

Guilherme Ramires

MTCNA, MTCWE, MTCRE, MTCTCE, MTCINE, MTCUME
MikroTik Official Consultant
MikroTik Certified Training Partner

ramires@alivesolutions.com.br

Alive Solutions & Voz e Dados
no MUM Brasil 2015



Tópicos a serem abordados

1. O MikroTik User Manager. Funções e possibilidades.
2. Instalando e configurando o User Manager
3. Hands On
4. Considerações finais





O MikroTik User Manager

O User Manager é um sistema de gestão de usuários baseado em RADIUS com diversas funcionalidades.

Pode ser usado para gerenciar usuários de:

- HotSpot
- PPP (PPTP, L2TP, PPPoE, etc)
- DHCP
- Wireless
- RouterOS

Funciona em processadores x86, ou RouterBoards com MIPS, PowerPC e TILE.

A RouterBoard deve ter pelo menos 32 MB de RAM e 2 MB de espaço livre no HD

É compatível com os principais navegadores de internet: Opera, Mozilla Firefox, Microsoft Internet Explorer e Safari.



O MikroTik User Manager

Cenário

Um WISP tem geralmente uma equipe grande e muitas RouterBoards em funcionamento.

A contratação e demissão de técnicos acontece constantemente. Como adicionar, alterar ou retirar acesso dos técnicos aos equipamentos imediatamente?

Utilizando o User Manager podemos fazer isso facilmente.



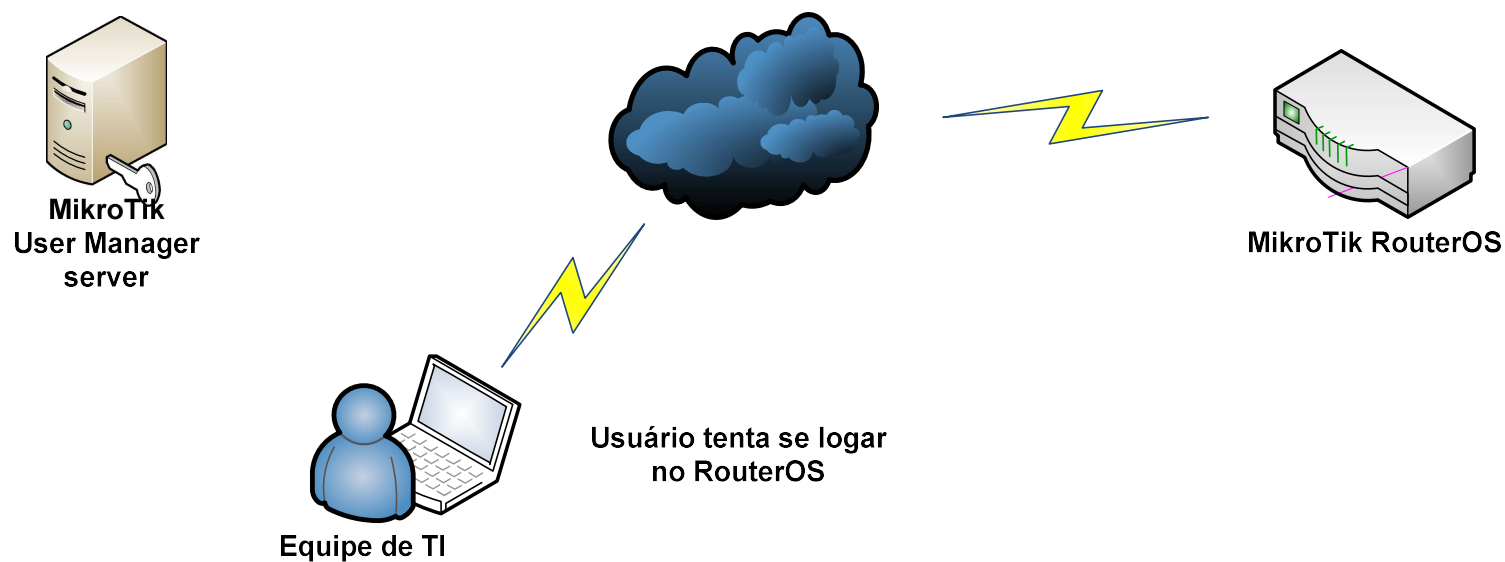
Nosso objetivo

- Melhorar a segurança de acesso aos MikroTik da rede e facilitar a adição e remoção de privilegio de acesso.
- Gerenciar clientes PPPOE, VPN, Wireless e Hotspot para provedores pequenos.



Como tudo acontece...

1. Usuário da equipe de TI tenta acessar um Router da rede (RouterOS).



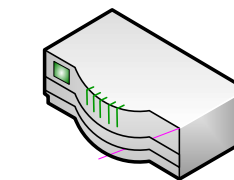


Como tudo acontece...

2. O router que o usuário está tentando logar consulta o User Manager.
3. O User Manager confirma a identidade do usuário.

UserManager confirma
identidade do usuário

RouterOS busca informações
no UserManager



MikroTik RouterOS

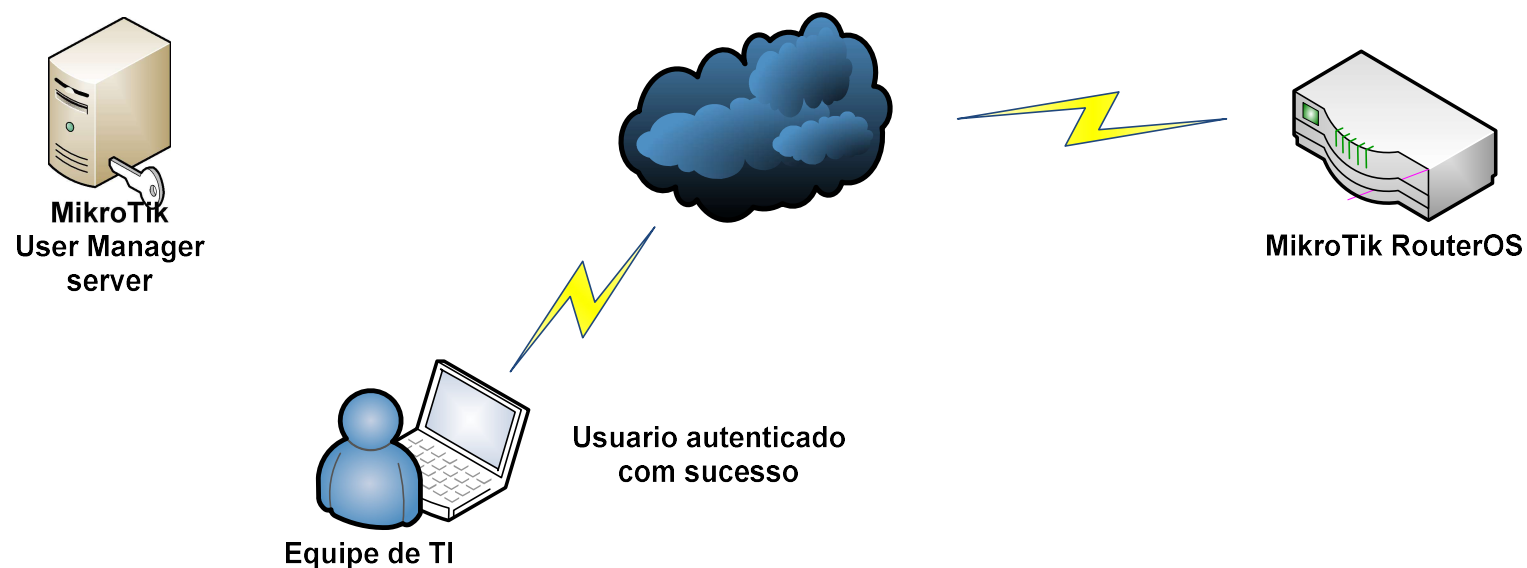


Equipe de TI



Como tudo acontece...

4. Usuário da equipe de TI autenticado com sucesso no MikroTik.





Instalando o User Manager





Instalando o User Manager

A Instalação do User Manager é simples.

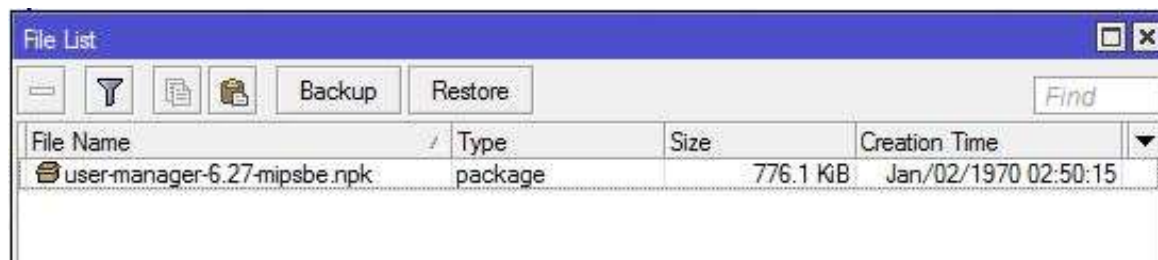
- Acesse o site da Mikrotik: <http://www.mikrotik.com/download>
- Faça download do pacote: **All packages**

v6.27	2015-Feb-23	
	Upgrade package	Standard upgrade package. Can also be used for Netinstall.
	All packages	Package with all features including less used ones.
	Wireless CAPsMANv2	Wireless test package which includes the new CAPsMAN feature (Controlled AP system manager).
	Netinstall	Utility for installation from network.
	Changelog	View changes in current version.
	MD5	View MD5 hashes to confirm file validity.



Instalando o User Manager

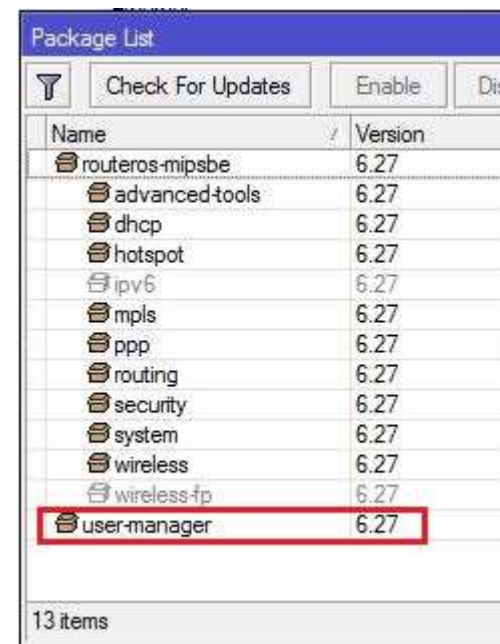
- Descompacte o pacote e copie para a RouterBoard o pacote do User Manager e a reinicie.



Dica:

Para o User Manager instalar é preciso que seja a mesma versão do RouterOS instalado em sua RouterBoard.

Caso não seja, atualize seu RouterOS.





Configurando o User Manager



12



Configurando o User Manager

Acima da versão 3.0 o User Manager já vem com o usuário padrão criado:

User: admin

Pass: em branco

É interessante mudar essa senha imediatamente:

```
/tool user-manager customer set admin password=12344321
```

Pela interface web podemos fazer toda configuração do User Manager.

Acesse : <http://ip-do-User Manager/userman>

Use as credenciais para acesso:

User: admin

Pass: 12344321

The screenshot shows the MikroTik User Manager web interface. At the top, the MikroTik logo and 'Mikrotik User Manager' text are displayed. Below this, there are two input fields: 'Login' and 'Password'. The 'Login' field contains the text 'admin'. Below the 'Password' field is a 'Log in' button.

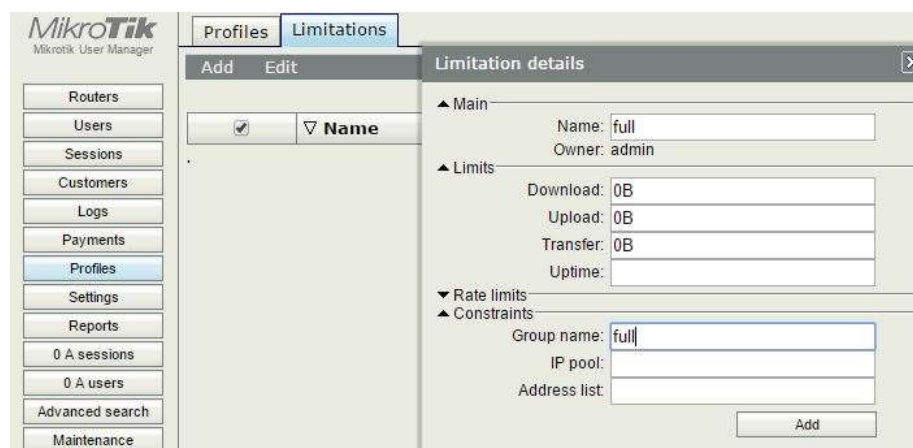


Configurando o User Manager

Primeiramente precisa criar o perfil e as limitações que ira disponibilizar para os técnicos.

São essas limitações que irão definir os direitos de cada usuário ao logar no MikroTik.

No exemplo usei o grupo: full.



- Defini um profile com nome: infra-admins
- Adicionei uma limitação de nome: full e no campo: Group name coloquei o nome do group que está no RouterOS no caso: full

14



Configurando o User Manager

Associando limitação ao profile: infra-admins

Clique no botão **Add new limitation** e selecione a limitação criada anteriormente: **full**

The screenshot shows the MikroTik User Manager web interface. The 'Limitations' tab is selected, and the profile 'infra-admins' is chosen. The 'Profile part' dialog box is open, showing the following configuration options:

- Period:**
 - Days: ☒ Sunday, ☒ Monday, ☒ Tuesday, ☒ Wednesday, ☒ Thursday, ☒ Friday, ☒ Saturday
 - Time: 0:00:00 to 23:59:59
- Limits:**
 - ☒ full
 - ☐ read

Buttons at the bottom of the dialog: New limit, Cancel, Add.

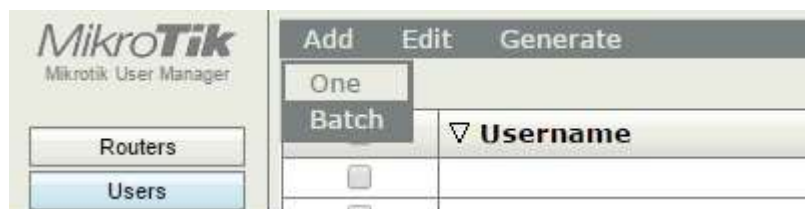
Observe que é possível definir dia da semana, e horário para uso do grupo de acesso.



Configurando o User Manager

Esses usuários criados no User Manager serão capaz de acessar todas as RouterBoards da rede configuradas.

Criando usuários para acessar seus MikroTik RouterOS:



Usando a interface web, vá no botão:

Users - Add – One

Assign profile: Define o profile do usuário.

Essas permissões podem ser alteradas a qualquer momento.

Shared user: Quantas conexões simultâneas o usuário poderá fazer.

16

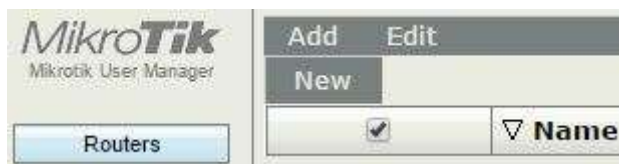


Configurando o User Manager

Para que o User Manager responda as requisições das RouterBoards é preciso cadastrá-las no NAS (network access server). Por segurança esse cadastramento deve ser feito com o IP de origem do MikroTik e uma senha, que deve estar configurada no router e no User Manager.

Pela interface web, acesse o botão:

Routers – Add - New



Router details

▲ Main

Name: router-01
Owner: admin
IP address: 10.0.0.1
Shared secret: 12345
Time zone: Parent time zone
Disabled: ☐
☐ Authorization success
☒ Authorization failure
Log events: ☐ Accounting success
☐ Accounting failure

▲ Radius incoming

CoA support: ☒ Use CoA
CoA port: 1700

Add



Configurando o User Manager

Pelo New Terminal esse trabalho é mais fácil. Você pode fazer um script adicionando todas suas RouterBoards de uma só vez.

DICA:

Para edição de scripts recomendo o aplicativo gratuito: Notepad ++

```
tool user-manager
router add ip-address=10.0.0.1 shared-secret=12345 coa-port=1700 customer=admin name=router-01
router add ip-address=10.0.0.2 shared-secret=12345 coa-port=1700 customer=admin name=router-02
router add ip-address=10.0.0.3 shared-secret=12345 coa-port=1700 customer=admin name=router-03
router add ip-address=10.0.0.4 shared-secret=12345 coa-port=1700 customer=admin name=router-04
```



Configurando o Router

As configuração a seguir deverão ser feita nos equipamentos da rede que serão acessados via usuários do User Manager

Em Radius Server cadastre o servidor que responderá as requisições Radius, (User Manager).

Configure aqui a senha que definimos em Routers no NAS do User Manager.

```
/radius
```

```
add address=10.0.0.254 secret=12345 service=login
```



Configurando o Router

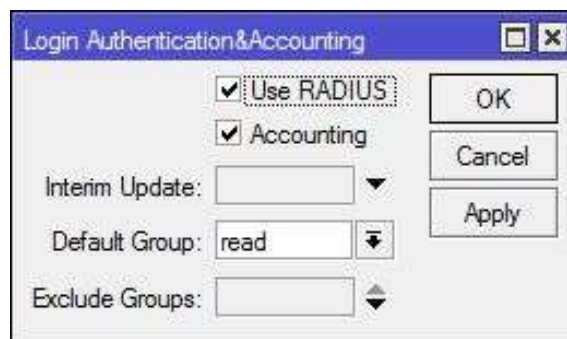
Em System - Users no botão AAA (Authentication, Authorization, and Accounting), configure para utilizar Radius.

Existem 2 campos nessa janela que gostaria de comentar:

Default Group – define qual grupo um usuário deve pertencer, caso o grupo que ele esta cadastrado no Radius não esteja configurado local no MikroTik.

Exclude Groups – usado para excluir um grupo que você não quer permitir logar nesse MikroTik com as permissões configuradas. Se configurarmos um grupo com permissões full se o Default Group estiver definido como read o usuário desse grupo terá permissão apenas para leitura.

```
/user aaa  
set use-radius=yes
```



20



Configurando o router

Lista de políticas permitidas:

local - política que concede os direitos para efetuar login localmente via console

telnet - política que concede direitos a logar-se remotamente via telnet

ssh - política que concede direitos a logar-se remotamente através do protocolo Secure Shell

ftp - política que concede plenos direitos para logar-se remotamente via FTP e transferir arquivos de e para o roteador. Os usuários com esta política podem ler, escrever e apagar arquivos, independentemente da permissão " read/write ", que lida apenas com configuração RouterOS.

reboot - política que permite reiniciar o roteador

read - política que concede acesso de leitura a configuração do roteador. Todos os comandos do console que não alteram a configuração do roteador são permitidos. Não afeta o FTP

write - política que concede acesso a escrever configuração do roteador, exceto para gerenciamento de usuários. Esta política não permite ler a configuração, por isso certifique-se de permitir assim a política de leitura

policy - política que concede direitos de gerenciamento de usuários. Deve ser usado em conjunto com a política de gravação. Permite também para ver as variáveis globais criadas por outros usuários (requer também a política 'test').

test - política que concede os direitos para executar ping, traceroute, bandwidth-test, wireless scan, sniffer, snooper e outros comandos de teste.

web - política que concede direitos a logar-se remotamente via WebBox

winbox - política que concede direitos a logar-se remotamente via WinBox

password - política que concede direitos para alterar a senha

sensitive - concede direitos para ver informações sensíveis no roteador, Como senhas salvas no MikroTik como: wireless, etc.

api - concede direitos para acessar roteador via API.

sniff - política que concede direitos de usar a ferramenta packet sniffer.

21



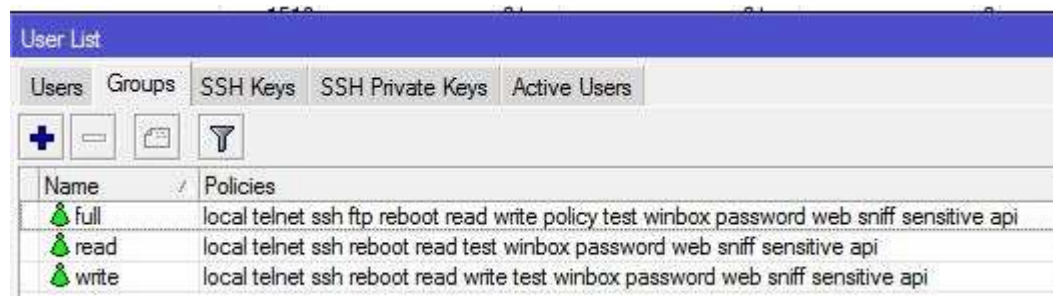
Configurando o router

System / Users

O Mikrotik RouterOS vem com grupos de segurança de usuários pré definidos (full, read, write)

Mas as permissões podem não ser adequadas ao seu negocio.

É interessante criar seus próprios grupos com permissões que se adaptem melhor ao seu cenário.



Name	Policies
full	local telnet ssh ftp reboot read write policy test winbox password web sniff sensitive api
read	local telnet ssh reboot read test winbox password web sniff sensitive api
write	local telnet ssh reboot read write test winbox password web sniff sensitive api



New Group

Name:

OK Cancel Apply Comment Copy Remove

Policies:

☒ local	☐ telnet
☒ ssh	☐ ftp
☐ reboot	☒ read
☐ write	☐ policy
☒ test	☒ winbox
☐ password	☐ web
☒ sniff	☐ sensitive
☐ api	

Skin:

System



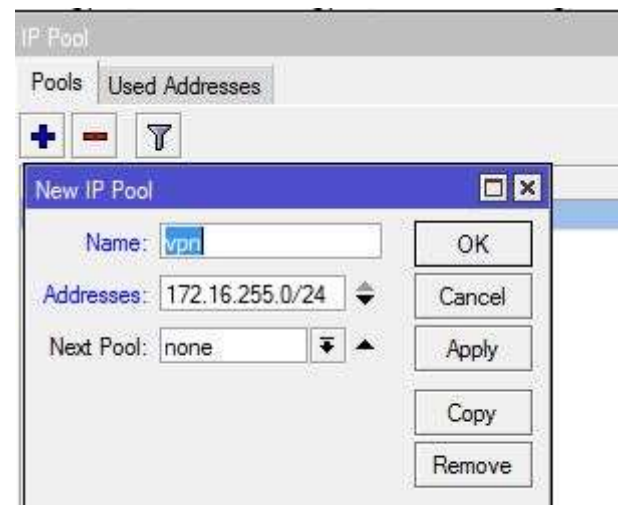
Servidor VPN ou PPPoE autenticando no User Manager

Primeiramente criamos um Pool de endereços que a VPN server ou o PPPoE server usarão para atribuir aos clientes que autenticarem no MikroTik.

Defini o range 172.16.255.0/24.

DICA:

Para fins de emergência, sugiro criar em cada equipamento um usuário com uma senha de poder do gerente de TI ou proprietário. Restrito a acesso local (Winbox MAC ou MAC Telnet), caso o equipamento esteja desconectado da rede e não consiga autenticar via User Manager.



```
/user
```

```
user add address=1.1.1.1/32 comment="support local" group=full name=support.local password=12344321
```



Configurando servidor

VPN ou PPPoE

The 'New PPP Profile' dialog box is shown with the 'General' tab selected. The 'Name' field is set to 'vpn'. The 'Local Address' is '10.0.0.254' and the 'Remote Address' is 'vpn'. Other fields like Bridge, Bridge Port Priority, Bridge Path Cost, Incoming Filter, Outgoing Filter, Address List, DNS Server, WINS Server, and Change TCP MSS are also visible.

Configure o Profile, definindo um nome um endereço local e selecione o pool criado anteriormente.

Em Protocols - Use Encryption select required para forçar a criptografia.

The 'New PPP Profile' dialog box is shown with the 'Protocols' tab selected. The 'Use Encryption' option is set to 'required'. Other options like 'Use MPLS', 'Use Compression', and 'Use VJ Compression' are also visible.



Configurando servidor VPN

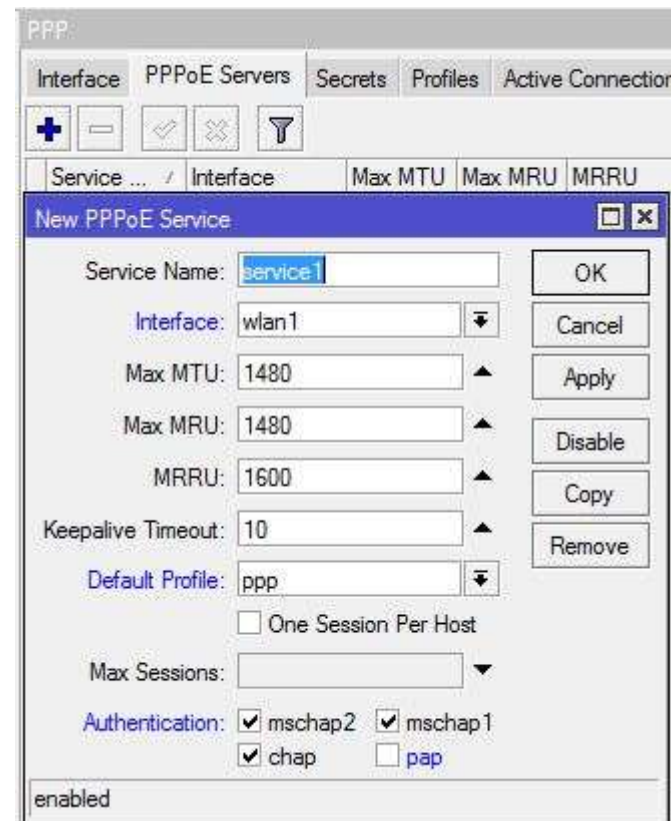
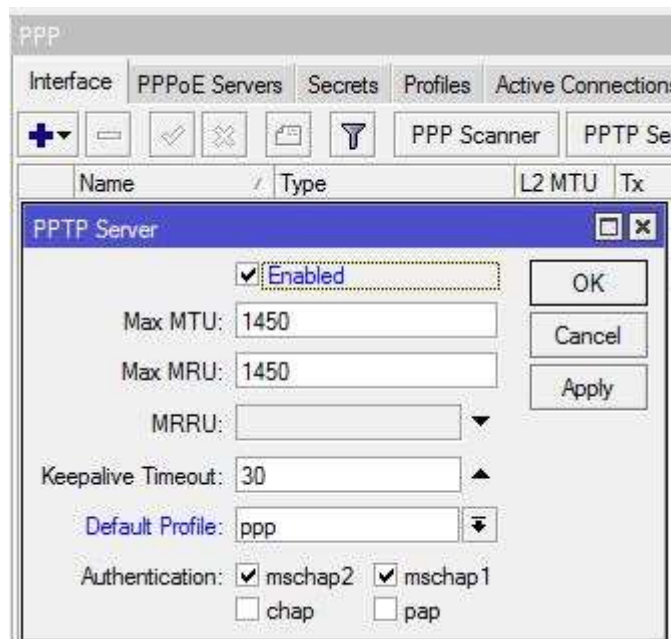
Em Secrets / PPP Authentication selecione Use Radius, para que o MikroTik utilize os usuários do User Manager.

- Para habilitar o VPN server, vá na aba Interface e clique no botão PPTP Server.

Selecione Enable e selecione o Profile criado anteriormente.

- Para habilitar o PPPoE server vá na aba PPPoE server e clique no botão +.

Selecione a interface e o perfil criado anteriormente.





Configurando servidor

VPN ou PPPoE

Finalizando, altere o perfil do servidor Radius que foi criado anteriormente habilitando ppp na autenticação Radius.

The screenshot shows the 'Radius Server <10.0.0.254>' configuration window. The 'General' tab is active. The 'Service' section has checkboxes for 'ppp' (checked), 'login' (checked), 'hotspot', 'wireless', and 'dhcp'. Below this are fields for 'Called ID', 'Domain', 'Address' (10.0.0.254), and 'Secret' (12345). The 'Authentication Port' is 1812 and the 'Accounting Port' is 1813. The 'Timeout' is 300 ms. There is an unchecked checkbox for 'Accounting Backup'. The 'Realm' field is empty, and the 'Src. Address' is 0.0.0.0. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', and 'Reset Status'. At the bottom left, the status is 'enabled'.

26



Configurando servidor VPN ou PPPoE

Usuário conectado na VPN.

PPP						
Interface PPPoE Servers Secrets Profiles Active Connections						
	Name	Service	Caller ID	Encoding	Address	Uptime
R	 read-support	pptp	192.168.107.254	MPPE128 stateless	172.16.255.255	00:00:43



Hands on



28



Hands on coletivo

Precisamos da ajuda de algumas pessoas do auditório para testarmos...

1. Conecte-se a rede wi-fi: **UserManager-lab**
2. Senha wi-fi: **floripa2015**
3. Use seu Winbox e conecte-se ao IP: **10.1.1.1**

Usuário: suporte

Senha: 12345

4. Observe as permissões concedidas.
5. Agora conecte-se com:

Usuário: infra-adm

Senha: 12345

6. Observe as permissões concedidas.



29

Dúvidas



Considerações finais

- **Gerência centralizada do pessoal técnico.**
- **Fácil de adicionar, bloquear ou remover usuários.**
- **Facilidade para mudar permissões de acesso dos técnicos.**
- **Montando grupos de segurança personalizados, é possível dar permissões específicas para técnicos com mais ou menos poder dentro da rede. Evitando assim dores de cabeça com técnicos de má intensão.**
- **Gratuito e eficiente. Basta instalar, configura-lo e pronto!!!**

Fonte

wiki.mikrotik.com





VALEU GALERA!



Anderson Marin Matozinhos

MTCNA, MTCWE, MTCRE, MTCTCE, MTCINE, MTCUME
MikroTik Official Consultant
MikroTik Certified Training Partner

anderson@icorporation.com.br

Guilherme Ramires

MTCNA, MTCWE, MTCRE, MTCTCE, MTCINE, MTCUME
MikroTik Official Consultant
MikroTik Certified Training Partner

ramires@alivesolutions.com.br

33