Olá, Cliente amigo,

Neste tutorial vamos descrever todos os passos de como fazer a integração do MK Auth com seu Mikrotik utilizando VPN.

Sem muitas delongas, vamos ao tutorial, lembrando que se fizer todos os passos com atenção, no final seu Mikrotik estará Integrado com o MK-Auth na nossa Nuvem.

Para começar, abra o e-mail que enviamos para você com os dados da VPN e sua RB e a interface WebAdmin do Mk-Auth. Abaixo estão o passo-a-passo:



New Interface				
	al Out Status Tra	affic		OK
Name:	VPN-MK-AUTH	5⁰		Cancel
Type:	L2TP Client			Apply
Actual MTU:				Disable
Max MTU:	1450			Comment
Max MRU:	1450		•	Сору
				Remove
				Torch
enabled		running	slave	Status:

4º Na nova tela clique na aba "General";

5º Coloque o nome da sua nova Interface, sugerimos "VPN-MK-AUTH";

New Interface	
General Dial Out Status Traffic	ОК
Connect To: mkauth.apptele.net 79	Cancel
User: telecomnuvem1 89	Apply
Password: ****** 92 •	Disable
Profile: default-encryption	Comment
Keepalive Timeout: 60	Сору
Dial On Demand Add Default Route Default Route Distance: 1 Allow: V mschap2 V mschap1 V chap V pap	Remove
enabled running slave S	itatus:

Interface <VPN-MK-AUTH> General Dial Out Status Traffic OK Last Link Down Time: Cancel Last Link Up Time: Sep/05/2022 10:36:05 Apply Link Downs: 0 Disable Uptime: 00:00:24 Comment Encoding: MPPE128 stateless Copy MTU: 1450 Remove MRU: 1450 Torch 10º Local Address: 172.31.255.10 Remote Address: 172.31.255.1 110 Status: connected enabled running

Session: D4:CA:6D:07:7B:9C Safe Mode ĺΩ. \mathbf{C} 🖋 Quick Set CAPsMAN 13 Interfaces Wireless Profiles Active Connections Secrets Interface PPPoE Servers L2TP Secrets Bridge 14º PPP Authentication&Accounting ♣||--4.5 12º 👍 PPP Caller ID Name Password Service Profile Local Addres C Switch 📲 Mesh PPP Authentication&Accounting 255 IP 15º Use Radius MPLS Þ 0K 乎 IPv6 Þ Accounting Cancel 对 Routing Þ Use Circuit ID in NAS Port ID Apply System 🖉 \mathbb{N} Interim Update: 00:03:00 🙅 Queues **6**⁰ 📄 Files 🗏 Log RADIUS

6º Clique na aba "Dial Out";

7º Coloque o endereço do servidor que enviamos para seu e-mail;

8º Coloque o usuário da VPN que está no email que enviamos;

9º Coloque a senha da VPN que enviamos no e-mail;

OBS: no e-mail que enviamos existe 10 VPNs, usar uma para cada RB, (Não pode usar VPN iguais para mais de uma RB);

Caso necessite de mais usuários solicite ao suporte técnico.

Clique em Apply para aplicar e salvar.

Na aba Status:

Confirme se a conexão foi realizada com sucesso, Status no rodapé deve ser: **conenected**

- 10^o Anote o Local Address (IP Local);
- 11^o Anote o Remote Address (IP Remoto);

- 12º Clique no "PPP";
- 13º Clique na Aba "Secret";

14⁰ Clique em "PPP Authentication&Accountig"

15º Na nova tela que abriu, marque a caixa "Use Radius";

16º Altere para "00:03:00" (No caso 3 minutos);

Clique em Apply para salvar.

Ativando o SNMP (monitoramento da RB):

ら CM Safe Mode	Session: D4:CA:6D:07:7B:9	C	
💓 Quick Set			
CAPsMAN			
Interfaces		SNMP Settings	
Wireless		✓ Enabled	199 ок
👯 Bridge		Contact Info: Telecom Nuvem	Cancel
🛓 PPP		Location: Brasil	
🙄 Switch			Арріу
°T° Mesh		Engine ID:	Communities
<u>₩</u> ₽ 179 [⊳]	ARP	Trap Target:	↓
O MPLS ►	Accounting	Trap Community: public	
🖞 IPv6 🗈	Addresses	Trap Version: 1	
Conting P	Cloud		
🔯 System 🗅	DHCP Client	Trap Generators: temp-exception	₹
🙅 Queues	DHCP Relay	Trap Interfaces:	≑
Files	DHCP Server	Src. Address: ::	
🗒 Log	DNS		
RADIUS	Firewall		
🗙 Tools 🛛 🗅	Hotspot	SNMP Communities	
🔤 New Terminal	IPsec	+ - ~ × - 7	Find
Dot 1X	Kid Control	Name Addresses	Security Read Ac Write Acc 🔻
MetaROUTER	Neighbors	* 🜔 public 172.31.255.1	20º none yes no
🤚 Partition	Packing		
Nake Supout.rif	Pool	SNMP Community <public></public>	
New WinBox	Routes	Name: public	ОК
🛃 Exit	SMB	Addresses: 172.31.2	255.1 21 9 ♦ Cancel
	SNMP 189	Security: none	
Windows 🔊	SSH	Read	Access
	Services	V head	Disable
	Settings		Access
	Socks	Authentication Protocol: MD5	Ţ
	TFTP	Encryption Protocol: DES	Сору
	Traffic Flow		Remove
Xo	UPnP	Authentication Password:	
B	Web Proxy	Encryption Password:	
VII		NUVEIV	
		enabled	default
õ			

17^o Clique em "IP";

18º Clique em "SMNP";

19º Na tela que vai abrir marque a opção "Enabled" e altere os dados de contato (opcional) e clique em Apply para salvar;

20º Na tela que vai abrir clique 2 vezes no "Public";

21⁰ Na tela que vai abrir Altere o "Addresses" para o ip do "Remote" que vimos no passo 11 e clique em Apply para Salvar.

Ativando o Radius (autenticação remota dos clientes PPPoE/Hotspot) no Mk-Auth:

	O MPLS ►		
	🛒 IPv6 🛛 🗅	BADIUS	
	Routing N		
	🔯 System 🗅		
	🙅 Queues	# Service Called ID	Domain Address Protocol 5
	📄 Files	New BADILIS Server	
	🗏 Log	Consult or a	
	RADIUS 229	General Status	ОК
	🗙 Tools 🛛 🗅	Service: 🗸 ppp 🛛 🔽 login	Cancel
	New Terminal	hotspot 🗸 wirele	ess Apply
	Oot1X	Z4º ✓ dhcp □ ipsec	c
	MetaROUTER	dot 1x	Disable
	Malua Supert of		Comment
		Called ID:	Сору
		Domain:	
		25º Address: 172.31.255.1	
	Windows	Protocol: udp	₹ Neset Status
		26º Secret: *****	
		Authentication Port: 1812	
		Accounting Parts 1912	
			ms
Xo		Accounting Back	up
B		Realm:	
Nil		Certificate: none	Ŧ
S		Src. Address: 0.0.0.0	
5			
te			
OL		enabled	
R.			

22⁰ Clique em "Radius";

23⁰ Na tela que vai abrir, clique no sinal "+";

24⁰ Marque as opções que mais lhe atende, normalmente PPPoE (se marcar todos não tem problema);

25° Informe o ip Remote que foi visto no passo 11;

26° Informe uma senha para o "Secret" e anote a mesma pois irá usar no MK-Auth

27º Altere o valor para 900;

Clique em Apply para Salvar

RADIUS	
🛉 🖃 🖉 Reset Status Incoming 289	Air
# Service Called ID Domain Address Protocol Secret Certificate 0 ppp login hotspot wirel 172.31.255.1 udp *****	28
RADIUS Incoming □ X 29º VAccept OK	29
Port: 3799 Cancel Requests: 0 Apply	Cli
Bad Requests: 0 Reset Status	
Naks: 0	
1 item	-1

Ainda dentro de Radius:

28⁰ Clique em "Incoming";

29⁰ Marque a caixa "Accept";

Clique em Apply para Salvar

Configurações no Mikrotik realizadas com sucesso, agora vamos ao Mk-Auth

Acesso seu MK-Auth na área de administrador (WebAdmin):

¢.	📥 PROVEDOR 🗸	📽 opções 🗸	📽 CLIENTES 🗸	\$ FINANCEIRO 🗸	🖨 SUPORTE 🗸	CENTRAL
CON	NFIGURAÇÕES 30º			CADASTROS		
> B	ackup do sistema			> Controle de	funcionarios	-
> C	ontas bancarias			> Controle de	ramais [servidores]	32º
> D	ados do provedor			> Controle de	planos	
> R	egistro do sistema			> Controle de	usuarios	
> P.	ainel do sistema			> Controle de	pool	
> G	erar Anatel DICI			> Controle de	produtos	
> V	Vebterminal shell			> Controle de	fornecedores	

Nenhum aviso novo...

- 30° Clique em "Provedor";
- 31º Clique em "Controle de Cadastros" somente versões mais antigas;
- 32º Clique em "Controle de Ramais [servidores]";



33^o Clique no "+" para adicionar um novo Servidor Mikrotik;

Por padrão o Mk-Auth já vem com um servidor cadastrado, você pode remover ou editar o mesmo se preferir.

IF do WK:	172.31.255.	10	34º	
Nome:	MikroTik		35º	
Тіро:	servidor - p	c ~	, 36º	
Senha mkauth:	•••••	37º		
Max. clientes:	1000			
Megas instalados:	99			
IP FALLBACK:	IP para aces	so rem	oto	
ncentrador dados Radius:				
Secret:	123456	389	2	
centrador acesso SNMP:				
Community:	public	E()	:OV	Ľ
#ID PLACA:	1	Ν	UVEN	
centrador acesso SSH:				
SSH Ativo:	⊙ Sim ⊖ I	Vão	39º	
Porta SSH:	22		40º	
centrador acesso FTP:				
FTP Ativo:	⊙ Sim	Não	41º	

Na tela de cadastro:

34⁰ Informe o ip do Local que vimos no passo 10º;

35º Informe uma descrição para sua RB para identificar a mesma;

36º Nesse passo é muito importante, pois nele precisa informar qual tipo de Mikrotik o MK Auth vai se conectar, se é um Servidor PC ou Uma RB;

Se for concentrador PPPoE selecione Servidor PC, se for um AP (wi-fi) selecione transmissor-RB

37º Informe uma senha segura (Essa será a mesma senha que iremos informar na criação do usuário dentro do Mikrotik);

38º Informe a senha do "Secret" (essa é a mesma senha informada no passo 26º) Não deixe a padrão 123456 pois irá comprometer a segurança do seu Radius,

39º Marque a opção "Sim" do SSH Ativo;

40º Informe o número da porta do SSH de seu Mikrotik (Caso tenha personalizado o número da porta lá no mikrotik, favor a informar aqui);

41º Marque a opção "Sim" do FTP;

Clique em Gravar no final da página;

42° Clique em "Chave SSH";

Isso irá fazer um Download de uma chave do MK-AUth, essa chave precisa ser copiada e colocada dentro do Mikrotik;

Após fazer o download da chave, volte para o Mikrotik;

🛒 IPv6 🛛 🗅	
📑 Routing 🗈	
🔯 System 🗈	File Cloud Backup 449
Queues 1 2 0	Restore Upload Find
Files	
🚊 Log	I chave pub 459 ssh key 30
RADIUS	directory
🔀 Tools 🛛 🗅	
🔤 New Terminal	
Dot 1X	•
MetaROUTER	2 items 18.4 MiB of 128.0 MiB used 85% free
Partition	

Copie a chave que baixou do mk-auth dentro do Windows.

43º Clique em "Files";

44⁰ Na nova tela, clique no ícone da prancheta (colar);

45° A chave que foi baixada no mk-auth tem que aparecer na lista;

🔯 System 🗈	Auto Upgrade					
Queues 469	Certificates					400
Files	Clock 10	O User List				46° Clique em "System"
🗮 Log	Console 40	Users Groups SSI	H Keys SSH Private Keys Activ	e Users		1 5
RADIUS	Disks 10	o 🕂 — 🖌 🗙	🗖 🍸 AAA			400
🔀 Tools 🛛 🗅	History	Name / Grou	ID Allowed Address	Last Logged In		48º Clique na aba "Users":
🔤 New Terminal	Identity	å brwifimk full		Lust Logged III	Sep/05/2022 10:41:46	
🚸 Dot1X	LEDs					
MetaROUTER	License		New Hear			49º Clique no sinal "+"·
🤔 Partition	Logging		500			
Make Supout.rif	Note		JU- Name: mkauth		ОК	
🔘 New WinBox	Packages		51º Group: full	₹	Cancel	50º Informe o usuário para o MK-
🛃 Exit	Password		Allowed Address:	\$	Apply	
	Ports		Last Logged In:		7 epiy	Auth acessar o Mikrotik. (OBS: para
💻 Windows 🛛 🗅	Reboot		520		Disable	
	Reset Configuration		JZ-Password:		Comment	runcionar, oprigatoriamente o
	Resources	539	Confirm Password:		Carry	usuário tem que ser "mkauth", tudo
	RouterBOARD				Сору	
	SNTP Client				Remove	junto e minusculo, se não for dessa
	Scheduler	1 item (1 selected)			Expire Password	forma não irá funcionar):
<	Scripts	<u>, </u>				
ă	Shutdown					E 40
-	Special Legin		enabled	expired		51° Alterar o Group para "full":
47⁰	Users					- ····································
5 ··· L	watchuog					
É (I contraction of the second seco

52° Informe a senha que foi criada no passo 37°;

53° Confirme a senha que foi criada no passo 37°;

Clique em Apply para salvar, o usuário deverá aparecer na lista de usuário.

User List		. <u>5</u> 4⁰			
Users Groups	SSH Keys	SSH Privat	te Keys	Active U	sers
	ort SSH Key	55⁰			
User	Key Owner	r			
					1
Import SSH K	ey				
User: m	kauth 569	2 Ir	mport SS	H Key	
Key File: 🛃	nave.pub	F	Cance	el	
	57 <u>⁰</u>				



55° Clique em "Import SSH Key";

56º Informe o usuário criado antes (Lembrando que o usuário obrigatoriamente precisa ser "mkauth" tudo minúsculo e juntos);

57º Selecione a chave que foi baixada do MK-Auth;

Clique em Import SSH Key



58º De volta no MK-Auth, clique em Detalhes na página onde ficam cadastrado os Ramais / Servidores;

Comandos			
Reiniciar Mikrotik	Desligar servidor	Chave SSH	Teste SSH
C		59	^{9⁰} ≻_
	Sistema MK-AUTH 🔏 telecomnuvem@mk-auth		

59º Na página que vai se abrir, procure no final dela a tela acima clique em "Teste SSH";

Após enviar o teste SSH, volte para o Mikrotik;

West								
₽ ₽ 612▷	ARP							
O MPLS D	Accounting	Firewall	63	<u>0</u>				
🛒 IPv6 🛛 🗅	Addresses	Filter Rules	NAT	Mangle	Raw	Service Ports	Connections	Address L
🔀 Routing 🗈	Cloud					Deast Countain	(O Deast A	Countom
🔯 System 🗈	DHCP Client				0	Neset Counters	to nesel A	Counters
🙅 Queues	DHCP Relay		tion I		Src.	Address Dst. /	Address Poto.	Src. Port
Files	DHCP Server	0 X 38	drop t	teste	NA 030	J COM 55H 440	bucua	64º
🗒 Log	DNS							
RADIUS	Firewall 620							
🗙 Tools 🛛 🗅								
💵 New Terminal	IPsec							
🚸 Dot1X	Kid Control							
💻 MetaROUTER	Neighbors							
🦺 Partition	Packing							
Nake Supout.rif	Pool							
New WinBox	Routes		N.L.	1\/E	n /	BY		
🛃 Exit	SMB	•		JVE				
	SNMP	1 item						
🔲 Windows 🗈	SSH							
	Services							

61° Clique em "IP";

62° Clique em "Firewall";

63º Na página que vai se abrir, clique na aba "Filter Rules";

64º Se você fez todos os passos certo, nesse momento a chave que foi gerada no passo 60º deverá estar listada aqui, caso não esteja listada a comunicação não está ocorrendo, neste caso revise todos os passos e verifique o que faltou ou ficou de forma incorreta.

Pronto, integração concluída com sucesso.

Basta agora cadastrar os clientes no MK-Auth e os mesmos já estrão sendo autenticados pelo MK Auth (desative os logins em Secrets).

Caso tenha mais alguma dúvida, estamos à disposição (telecomnuvem.com.br)



Recomentamos também alguns passos adicionais de segurança, abaixo!

Alterar os serviços limitando o acesso pelo IP do Mk-Auth (SSH/FTP):

🙄 Switch							
T Moob							
🛤 IP 🗈 🗈	ARP						
тер Г	Accounting						
🛫 IPv6 🛛 🗅	Addresses	IP :	Service List				
🖈 Routing 🛛 🗅	Cloud		× 7				Find
🗊 System 🛛 🗅	DHCP Client	1	Name	/ Dort	Ausilable Emm	Cotificato	TI S Vor
💂 Queues	DHCP Relay	X	api	- FUIL 8728	Available FI0ITI	Certificate	TLS Ver +
📔 Files	DHCP Server	×	🛛 api-ssi	8725		none	any
Log	DNS		ftp	21	172.31.255.1		
RADIUS	Firewall		ssn	22			
🖌 Tools 🛛 🗅	Hotspot		winbox	8291			
🗷 New Terminal	IPsec	X	www	80			
Dot1X	Kid Control	×	WWW-SSI	443		none	any
🕂 MetaROUTER	Neighbors		10.0				
🖢 Partition	Packing		IP S	ervice ⊲tp>			
💫 Make Supout.rif	Pool			Name: ftp)		ОК
New WinBox	Routes			Port: 2	1		Cancel
🛃 Exit	SMB		Ava	ilable From: 1	72.31.255.1	\$	
	SNMP						Apply
💻 Windows 🛛 🗅	SSH	8 it	ems (1 se				Disable
	Services		• •	de d		-	
	Settings		enab	bied			
	Socks						
	тстр						

Uma das recomendações de segurança é que você limite o acesso as portas SSH e FTP do seu Mikrotik

Desta forma somente o Mk-Auth terá acesso as mesmas, para isso:

- 1º Vá em IP > Services
- 2º De dois cliques em FTP

Em Available From digite o IP do Mk-Auth da VPN, no nosso caso: 172.31.255.1

Clique em Apply para Salvar

No caso da porta SSH recomendamos ainda alterar a numeração da mesma, pra ficar menos exposta ainda, para isso altere em Port a numeração da mesma para por exemplo: 2022

Ao alterar a porta SSH não esqueça de alterar no cadastro do ramal/servidor lá no Mk-Auth



Alterar o usuário mkauth limitando o acesso pelo IP do Mk-Auth:

LA ROUTING			
🔯 System 🗅	Auto Upgrade		
	Certificates	lease 1 link	
Files	Clock		
🗒 Log	Console	Users Groups SSH Keys SSH Private Keys Active L	lsers
RADIUS	Disks	🕂 🗕 🖌 🗶 🗖 🏹 🗛	
🔀 Tools 🛛 🗅	History	Name / Group Allowed Address	Last Logged In
🔤 New Terminal	Identity	howifime full	Sep/05/2022 10:41:4
🚸 Dot1X	LEDs	👗 mkauth 🛛 full	Sep/05/2022 11:36:
💻 MetaROUTER	License		
🦺 Partition	Logging	User <mkauth></mkauth>	
📡 Make Supout.rif	Note	Name: mkauth	OK
🔘 New WinBox	Packages	Group: full	Cancel
🛃 Exit	Password	Allowed Address: 172.31.255.1	♦ Apply
	Ports	Last Logged In: Sep/05/2022 11:36:50	лфріу
Windows 🗅	Reboot		Disable
	Reset Configuration		Comment
	Resources		
	RouterBOARD		Сору
	SNTP Client		Remove
	Scheduler	2 items	Password
5	Scripts		
5	Shutdown		Expire Password
	Special Login	enabled expired	
	Users		
S .	watchdog		
1			

Outra recomendação é limitar o acesso do usuário mkauth pelo ip do mk-auth via VPN:

Desta forma somente este usuário só poderá ser utilizado se vier pelo IP da VPN:

1º Vá em System > Users

2º De dois cliques no usuário mkauth

Em Allowed Address digite o IP do Mk-Auth da VPN, no nosso caso: 172.31.255.1

Clique em Apply para Salvar

Também recomendamos que use sempre uma senha forte, e caso altere esta senha aqui deve alterar também no sistema mk-auth em ramais/servidores.

