

Configuração OpenVPN

R3005G e Mikrotik

Pós-Venda - Redes

22 de Dezembro de 2023

Sumário

1	Introdução	3
2	Configuração do Roteador Mikrotik:	3
3	Configuração do Certificado:3.1Criar Certificado CA3.2Criar e assinar o Certificado do Servidor3.3Crie e assine o Certificado Client3.4Exporte o Certificado de autoridade (CA)3.5Exporte o Certificado Client3.6Baixe os certificados	3 3 4 5 6 7
4	IP Pool4.1Configure IP Pool4.2Configure Profile PPP4.3Crie um usuário4.4Ative o Servidor OpenVPN	7 7 9 9
5	Configuração do R3005G5.1Informações do dispositivo5.2Faça o Upload dos certificados5.3Checando o status da conexão	10 10 10 11

1 Introdução

Foi identificado que o RouterOS 6.x da MikroTik possui algumas inconsistências no funcionamento do OpenVPN, e este precisa de alguns ajustes específicos para que o OpenVPN funcione adequadamente.

2 Configuração do Roteador Mikrotik:

· Informações sobre os modelos e versão dos dispositivos testados

RouterBOARD		
	✔ RouterBOARD	OK
Model:	RB750Gr3	Ungrade
Revision:	r4	Cattinga
Serial Number:	HCQ08CH7SEF	Settings
Firmware Type:	mt7621L	USB Power Reset
Factory Firmware:	6.48.6	Mode Button
Current Firmware:	6.48.6	Reset Button
Upgrade Firmware:	6.48.6	

RouterBOARD	
✓ RouterBOARD	ОК
Model: RB750Gr3	Upgrade
Revision: r4	Settinge
Serial Number: CC210D35FF41	UCD Dawing Daart
Firmware Type: mt7621L	USB Fower Reset
Factory Firmware: 6.47.6	Mode Button
Current Firmware: 6.49.10	Reset Button
Upgrade Firmware: 6.49.10	

3 Configuração do Certificado:

 Entre em System > Certificates > Certificates; Na Página de criação de certificados crie o CA, o certificado do Servidor e o certificado Client

3.1 Criar Certificado CA

 Lembre-se de colocar o IP de Wan do mikrotik onde as requisições de OpenVPN irão chegar ao assinar o certificado, pois o mikrotik em versões mais antigas podem ter alguns problemas para negociar os certificados se não houver esta informação.

New Certificate		Certificate <ovpnca></ovpnca>	
General Key Usage Status	OK	General Key Usage Status	OK
1 2 Name: OVPRCA	Cancel	Key Usage: _ digital signature _ content commitment	Cancel
Issuer:	Apply	key encipherment data encipherment	7 Apply
~	Сору	key agreement b key cert. sign c crl sign encipher only	Сору
Country:	Remove	decipher only dvcs	Remove
State:	Sign	🗌 server gated crypto 🗌 ocsp sign	8 Sign
Locality:	Sign via SCEP	timestamp ipsec user	Sign via SCEP
Organization:	Create Cert. Request	ipsec tunnel ipsec end system	Create Cert. Request
Unit:	Import	email protect code sign	Import
3 Common Name: ovpnCA	Card Reinstall	Sign	Card Reinstall
Subject Alt. Name:	Card Verify	Cartificata: ampCi I Start	Card Verify
Key Type: RSA	Export	10 Stop	Export
Key Size: 2048	Revoke	Ch CPU 19 100 160 100 177	Revoke
Days Valid: 365		Progress: Mikrotik WAN IP	
privat crl authority revoked expired smart	. trusted	privat [crl authority revoked expired smart	. trusted

Confirme se o Checkbox "Trusted" está marcado conforme abaixo:

Certificate <ovpnca< th=""><th>۷</th><th></th></ovpnca<>	۷	
General Key Usage	Status	OK
Name:	ovpnCA	Cancel
Issuer:	^	Apply
		Copy
Country	,	Remove
State:		Sign
Locality:		Sign via SCEP
Organization:		Create Cert. Request
Unit:		Import
Common Name:	ovpnCA	Card Reinstall
Subject Alt. Name:		Card Verify
Key Type:	RSA	Export
Key Size:	2048	Revoke
Days Valid:	365	
L	✓ Trusted	
private key crl	authority revoked expired smart card trus	ted

3.2 Criar e assinar o Certificado do Servidor

New Certificate		🗌 🗙 Certificate -	<pre><ovpnserver></ovpnserver></pre>			
General Key Usage Status	OK	General Ke	y Usage Status			ОК
2 Name: ovpnServer	Canc	el Key Usage:	digital signature	content commitm	ent	Cancel
Issuer:	App]	y 6 🖸	key encipherment	data encipherme	nt	8 Apply
	Cop	у	key agreement	key cert. sign		Сору
Country:	Remo	ve	decipher only	dvcs		Remove
State:	Sig	n	server gated crypt	o 🗌 ocsp sign		9 Sign
Locality:	Sign via	a SCEP	timestamp	ipsec user		Sign via SCEP
Organization:	Create Cert	. Request	ipsec tunnel	ipsec end syste	n	Create Cert. Request
Unit:	Inpo	rt	email protect	code sign		Import
3 Common Name: ovpnServer	Card Rei	nstall	tls client /	✓ tls server		Card Reinstall
Subject Alt. Name:	Card Ve	srify Si	gn			Card Verify
Key Type: RSA	Expo	rt C	ertificate: ovpnServ	rer 🛛 🔻 🛔 🔤	Start	Export
Key Size: 2048	₹ Revo	ke	10 CA: ovpnCA	─ ▼ ▲' '	Stop	Revoke
Days Valid: 365		c	A CRL Host:	\$	Close	
			Progress:			
privat crl authority revoked	expired smart trusted	privat cr	authority r	evoked expired	smart	trusted

Confirme se o checkbox "Trusted" está marcado, conforme abaixo:

Certificate <ovpnse< th=""><th>rver></th><th></th></ovpnse<>	rver>	
General Key Usage	Status	OK
Name:	ovpnServer	Cancel
Issuer:	^	Apply
	~	Сору
Country		Remove
State:		Sign
Locality:		Sign via SCEP
Organization:		Create Cert. Request
Unit:		Import
Common Name:	ovpnServer	Card Reinstall
Subject Alt. Name:		Card Verify
Key Type:	RSA	Export
Key Size:	2048	Revoke
Days Valid:	365	
	V Irusted	
private key crl	authority issued expired smart card trus	ted

3.3 Crie e assine o Certificado Client

New Certificate			Certificate (ovpmClient)	
General Key Usage Sta	atus	OK	General Key Usage Status	OK
1 2 Name: ovpr/	nClient	Cancel	Key Usage: _ digital signature _ content commitment	Cancel
Issuer:	^	ápply	key encipherment data encipherment	6 Apply
		Copy	key agreement key cert. sign	Copy
	*	Remove	crl sign encipher only	Renove
Country:			decipher only dvcs	
State:		Sign	server gated crypto ocsp sign	7 Sign
Locality:		Sign via SCEP	timestamp ipsec user	Sign via SCEP
Organization:		Create Cert. Request	ipsec tunnel ipsec end system	Create Cert. Request
Unit:		Import	email protect code sign	Import
3 Common Name: ovpn0	nClient	Card Reinstall	5 vils client tls server	Card Reinstall
Subject Alt. Name:	\$	Card Verify	Sign X	Card Verify
Key Type: RSA		Export	Certificate: ovpnClient T 9 Start	Export
Key Size: 2048	8 🛛	Revoke	8 CA: ovpnCA T A Stop	Revoke
Days Valid: 365			CA CRL Host:	
			Progress: done	
privat crl aut	thority revoked expired smart		private key [cr] authority issued expired smart card [trust	

Neste caso o checkbox "Trusted" está desmarcado, conforme abaixo:

Certificate <ovpncl< th=""><th>ient></th><th></th></ovpncl<>	ient>	
General Key Usage	Status	OK
Name:	ovpnClient	Cancel
Issuer:	A	Apply
	~	Сору
Country		Remove
State:		Sign
Locality:		Sign via SCEP
Organization:		Create Cert. Request
Unit:		Import
Common Name:	ovpnClient	Card Reinstall
Subject Alt. Name:		Card Verify
Key Type:	RSA	Export
Key Size:	2048	Revoke
Days Valid:	365	·
privete ker [22]	authovity issued avaiyad and in	ted

• Verifique se os 3 certificados foram criados corretamente

Certificates										
Certificate	s SCEP Servers	SCEP RA Request	s OTP CRL							
+ -	Import Card Reinstall Card Verify Revoke Settings									
	Name /	Issuer	Common Name	Subject Alt. N	Key Size	Days Valid	Trusted	SCEP URL	CA	Fingerprint
KLAT	ovpnCA		ovpnCA		2048	365	yes			42efad739e
KI	ovpnClient		ovpnClient		2048	365	no		ovpnCA	19c54ae363
KIT	ovpnServer		ovpnServer		2048	365	yes		ovpnCA	7422220341

3.4 Exporte o Certificado de autoridade (CA)

Certificate KovpnCA	>						
General Key Usage	Status					. [OK
1 Name:	ovpnCA						Cancel
Issuer:						^	Apply
	Ex	xport					Сору
Country:		Certif	icate: 💽	/pnCA	4 Export		Remove
State:			Type: PE	an a	Cancel		Sign
Locality:	I	Export Passp	hrase:		•		Sign via SCEP
Organization:		3 File	Name: Ov	/pnCA			Create Cert. Request
Unit:							Import
Common Name:	ovpnCA						Card Reinstall
Subject Alt. Name:							Card Verify
Key Type:	RSA						2 Export
Key Size:	2048						Revoke
Days Valid:	365						
	✔ Trusted						
private key crl	a	uthority	revoked	expired	smart card.	truste	d

3.5 Exporte o Certificado Client

Certificate <ovpnclient></ovpnclient>									
General Key Usage	Status					ОК			
1 Name: ovpn	Client					Cancel			
Issuer:					A	Apply			
E	Export					Сору			
Country:	Certificate: ovpnClie	nt 🔻	Export			Remove			
State:	Type: PEM	, [Cancel			Sign			
Locality:	Export Passphrase: 1234567					Sign via SCEP			
Organization:	File Name ovpnClie	<u>nt 4</u>				Create Cert. Request			
Unit:						Import			
Common Name: ovpn	Client					Card Reinstall			
Subject Alt. Name:	Guarde	a sent	na colo	cada ac	ni .	Card Verify			
Key Type: RSA	Guarac	u sem		cuuu ut	2	Export			
Key Size: 2048	3					Revoke			
Days Valid: 365									
Trusted									
private key Cri	authority	issued	expired	smart card key	trusted				

3.6 Baixe os certificados

File List			
File Cloud Backup			
😑 🍸 🗎 🔒 🖪 Backup	Restore Upload		Find
File Name	∇ Type	Size	Creation Time
🕘 ovpnClient.key	.key file	1858 B	Sep/01/2023 13:10:10
ovpnClient.crt	.crt file	1151 B	Sep/01/2023 13:10:10
ovpnCA.crt	.crt file	1188 B	Sep/01/2023 13:09:34
🧧 flash	disk		Jan/01/1970 22:26:41
🔤 flash/skins	directory		Feb/07/2106 03:28:24
🔚 flash/pub	directory		Oct/25/2021 15:37:19
☐ flash/log.0.txt	.txt file	13.7 KiB	Aug/03/2023 06:04:34
flash/auto-before-reset.backup	backup	28.5 KiB	Feb/07/2106 03:28:27

4 IP Pool

4.1 Configure IP Pool

• IP > IP Pool > novo Pool

IP Pool			
Pools Used Addresses	l		
+- 🗆 🍸			Find
Name (Adda	00000	Nov+ Pool	•
👕 default-d IP Pool <	ovpnPool>		
Vame Name	: ovpnPool	OK	
Addresses	: 10.0.0.10-10.0.0.20 🗘	Cancel	
Next Pool	: none ∓ 🔺	Apply	
		Comment	
		Copy	
		Remove	
2 items (1 selected)			
L TOOMS (I SCICCOOL)			

4.2 Configure Profile PPP

• PPP>Profiles

PPP Profile <ovpnprofile></ovpnprofile>	
General Protocols Limits Queue Scripts	ОК
Name: ovpnProfile	Cancel
Local Address: 10.0.0.1 🔾 🔺	Apply
Remote Address: ovpnPool 🗧 🔺	Comment
Bridge:	Сору
Bridge Port Priority:	Remove
Bridge Path Cost:	
Bridge Horizon:	
Bridge Learning: default	
Incoming Filter:	
Outgoing Filter:	
Address List:	
Interface List:	
DNS Server: 1.1.1.1 🗢	
8.8.8.8	
WINS Server:	
- Change TCP MSS	
Ono Oyes ⊙default	
- Use UPnP	
Ono Oyes ⊙default	

4.3 Crie um usuário

PPP Secret <teste></teste>		
Name:	teste	OK
Password:	12345678	Cancel
Service:	ovpn Ŧ	Apply
Caller ID:	•	
Profile:	ovpnProfile Ŧ	Disable
Local Address:	▼	Comment
Remote Address	▼	Сору
		Remove
Routes:	▼	
Limit Bytes In:	•	
Limit Bytes Out:	•	
Last Logged Out:	Sep/01/2023 14:50:20	
Last Caller ID:	10.100.26.167	
Last Disconnect Reason:	hung up	
enabled		

4.4 Ative o Servidor OpenVPN

PPP		
Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets	2	
+ V XX C Y PPP Scanner PPTP Server SSTP Server L2TP Se	rver OVPN Server PPPoE Scan	Find
Name / Type Actual MTU L2 MTU Tx	Rx Tx Packet (p/s) Rx Packet (p/s) FP Tx	FP Rx FP Tx Packet (p/s) FP Rx Packet (p/s)
	OVPN Server	
	3 Enabled OK	
	Port: 4443 Cancel	
	Mode: ip Apply	
	Netmask: 24	
	MAC Address: FE:50:C6:81:4A:31	
	Max MTU: 1400	
	Keepalive Timeout: 60	
	Default Profile ovpnProfile 4	
	Certificate ovpnServer 5 =	
0 items out of 5	G Require Client Certificate	
	Auth.: 🗹 sha1 🗌 md5	
	Cipher: blowfish 128 aes 128	
	aes 192 aes 256 7	

Feito isso, lembre-se de liberar no firewall para aceitar as requisições da porta 4443 ou a outra porta que for utilizar para o serviço

5 Configuração do R3005G

5.1 Informações do dispositivo



5.2 Faça o Upload dos certificados



- Configure os parâmetros do cliente OpenVPN conforme o cenário configurado em seu servidor OpenVPN com o secret configurado, senha e o IP do mikrotik que irá receber as requisições.
- É muito importante que o IP seja o mesmo IP configurado no certificado de autoridade do mikrotik, pois se estiver divergente, a sessão OpenVPN não será estabelecida.

intelbras ≡	Q. Busca de função
 Visão Geral Monitoramento 	Sistema < Flow control < Segurança < Comportamento < <u>VPN <</u> Avançado < Armazenamento USB Diagnóstico <
Interface	Configuração OVPN Usuário OVPN Certificado OVPN Estado OVPN Log OVPN
🖶 Roteador	A implementação da camada de aplicação VPN baseada na biblioteca OpenSSL tem a vantagem de simplicidade e facilidade de uso
Autenticação	Estado O Servidor O Cliente
🗮 Sistema	Protocolo TCP UDP
	Tempo limite de Keepalive(s) - 60 +
	Ativar TLS
	Cifra AES-256 *
	Autenticação SHA1 👻
	*MTU – 1400 +
	senha de chave privada 12345678 Senha usada para exportar o certificado client
	* Nome de usuário teste
	* Senha 12345678
	* Endereço do servidor 10.100.26.163:4443
	Cancelar modificação Salvar configuração

Lembre-se de colocar a mesma senha de chave privada configurada na exportação do certificado Client do mikrotik

5.3 Checando o status da conexão

A conexão deve subir entre 1 a 4 minutos

intelbras ≡	Q Busca de função			
📩 Visão Geral	Sistema V Flow control V Segurança V Comportamento VPN V Avançado V			
Ø Monitoramento	Armazenamento USB Diagnóstico ~			
☐ Interface	Configuração OVPN Usuário OVPN Certificado OVPN Estado OVPN Log OVPN			
Han Roteador	Estado OVPN Autenticação com certificados de terceiros			
Informações de estado				
Autenticação	Tempo de conexão Fri Sep 1 15:18:56 2023			
÷ Sistema	Enviar dados 7.60 KB			
	receber dados 7.40 KB			
	Endereço IP 10.0.0.20			
	Atualizar dados Reconecte Desconectar			

- Estas configurações são para funcionamento em cenários onde o OpenVPN server está rodando em routerOS 6.x
- Na versão do routerOS 7.x não é necessário especificar o IP de Wan dentro do certificado.

- As configurações feitas no RouterOS6.x funcionarão no routerOS7.x quando o mikrotik for atualizado para esta versão.
- Nota: podem ocorrer alguns logs de erros no mikrotik server quando o cliente openVPN estiver tentando a conexão, esses erros somente ocorrem na versão 6.x do routerOS. Aparentemente trata-se de um bug não tratado pela mikrotik

17	Freeze				Find	al	₹
#	Time	Buffer	Topics	Message			•
137	Sep/01/2023 14:53:51	memory	ovpn, info	TCP connection established from 10.100.26.167			+
138	Sep/01/2023 14:53:52	memory	ovpn, debug, error, unknown, unknown, unknown, unkn	duplicate packet, dropping			
139	Sep/01/2023 14:54:27	memory	ovpn, info	TCP connection established from 10.100.26.167			
140	Sep/01/2023 14:54:28	memory	ovpn, debug, error, unknown, unknown, unknown, unkn	duplicate packet, dropping			
141	Sep/01/2023 14:54:50	memory	ovpn, info	TCP connection established from 10.100.26.167			
142	Sep/01/2023 14:54:51	memory	ovpn, debug, error, unknown, unknown, unknown, unkn	duplicate packet, dropping			
143	Sep/01/2023 14:55:26	memory	ovpn, info	TCP connection established from 10.100.26.167			
144	Sep/01/2023 14:55:27	memory	ovpn, debug, error, unknown, unknown, unknown, unkn	duplicate packet, dropping			
145	Sep/01/2023 14:56:02	memory	ovpn, info	TCP connection established from 10.100.26.167			
146	Sep/01/2023 14:56:03	memory	ovpn, debug, error, unknown, unknown, unknown, unkn	duplicate packet, dropping			
147	Sep/01/2023 14:56:04	memory	ovpn, info	: using encoding - AES-256-CBC/SHA1			
148	Sep/01/2023 14:56:04	memory	ovpn, info, account	teste logged in, 10.0.0.20 from 10.100.26.167			
149	Sep/01/2023 14:56:04	memory	ovpn, info	<ovpn-teste>: connected</ovpn-teste>			
150	Sep/01/2023 15:02:17	memory	system, info, account	user admin logged out from 00:E0:4C:68:01:A1 via winbox			
151	Sep/01/2023 15:11:30	memory	system, info, account	user admin logged in from 00:E0:4C:68:01:A1 via winbox			
152	Sep/01/2023 15:25:38	memory	ovpn, info	<ovpn-teste>: terminating peer disconnected</ovpn-teste>			
153	Sep/01/2023 15:25:39	memory	ovpn, info, account	teste logged out, 1775 1392 1408 87 88 from 10.100.26.167			
154	Sep/01/2023 15:25:39	memory	ovpn, info	<ovpn-teste>: disconnected</ovpn-teste>			
155	Sep/01/2023 15:25:39	memory	ovpn, info	TCP connection established from 10.100.26.167			
156	Sep/01/2023 15:25:40	memory	ovpn, debug, error, unknown, unknown, unknown, unkn	duplicate packet, dropping			
157	Sep/01/2023 15:26:15	memory	ovpn, info	TCP connection established from 10.100.26.167			
158	Sep/01/2023 15:26:16	memory	ovpn, debug, error, unknown, unknown, unknown, unkn	duplicate packet, dropping			
159	Sep/01/2023 15:26:18	memory	ovpn, info	: using encoding - AES-256-CBC/SHA1			
160	Sep/01/2023 15:26:18	memory	ovpn, info, account	teste logged in, 10.0.0.20 from 10.100.26.167			
161	Sep/01/2023 15:26:18	memory	ovpn, info	<ovpn-teste>: connected</ovpn-teste>			+
162	items (1 selected)						

No RouterOS 7.x não ocorrem esses erros, a mesma configuração quando feita a atualização do routerOS 6.x para a versão 7.x funciona sem problemas, e sem os erros.

Log				
7	Freeze			
#	Time	Buffer	Topics	Message
0	Jan/01/1970 21:00:25	memory	system, info	installed system-7.11.2
1	Jan/01/1970 21:00:25	memory	system, info	crossfig will upgrade version 6 configuration
2	Jan/01/1970 21:00:25	memory	system, info	router rebooted
3	Jan/01/1970 21:00:29	memory	interface, info	ether1 link up (speed 1G, full duplex)
4	Jan/01/1970 21:00:29	memory	interface, info	ether2 link up (speed 1G, full duplex)
5	Jan/01/1970 21:00:29	memory	interface, info	ether3 link up (speed 1G, full duplex)
6	Jan/01/1970 21:00:31	memory	system, info, account	user admin logged in from 00:E0:4C:68:01:A1 via winbox
7	Jan/01/1970 21:00:35	memory	dhcp, info	dhcp-client on ether1 got IP address 10.100.26.163
8	Jan/01/1970 21:00:36	memory	ovpn, info	connection established from 10.100.26.167, port: 58286 to 10.100.26.163
9	Jan/01/1970 21:00:38	memory	ovpn, info	<10.100.26.167>: disconnected <tls (6)="" certificate="" error:="" not="" ssl:="" valid="" yet=""></tls>
10	Jan/01/1970 21:00:40	memory	route, ospf, info	instance { version: 2 router-id: 10.100.26.163 } created
11	Jan/01/1970 21:00:43	memory	ovpn, info	connection established from 10.100.26.167, port: 58288 to 10.100.26.163
12	Jan/01/1970 21:00:46	memory	ovpn, info	<10.100.26.167>: disconnected <tls (6)="" certificate="" error:="" not="" ssl:="" valid="" yet=""></tls>
13	Jan/01/1970 21:00:51	memory	ovpn, info	connection established from 10.100.26.167, port: 58292 to 10.100.26.163
14	Sep/01/2023 15:45:24	memory	system, critical, info	cloud change time Jan/01/1970 21:00:53 => Sep/01/2023 15:45:24
15	Sep/01/2023 15:45:24	memory	ovpn, info	: using encoding - AES-256-CBC/SHA1
16	Sep/01/2023 15:45:24	memory	ovpn, info, account	teste logged in, 10.0.0.20 from 10.100.26.167
17	Sep/01/2023 15:45:24	memory	ovpn, info	<ovpnteste>: connected</ovpnteste>

Suporte a clientes: (48)2106-0006 Fórum: forum.intelbras.com.br SAC: 0800 7042767