

intelbras

Sempre próxima

Configuração OpenVPN

R3005G e Mikrotik

Sumário

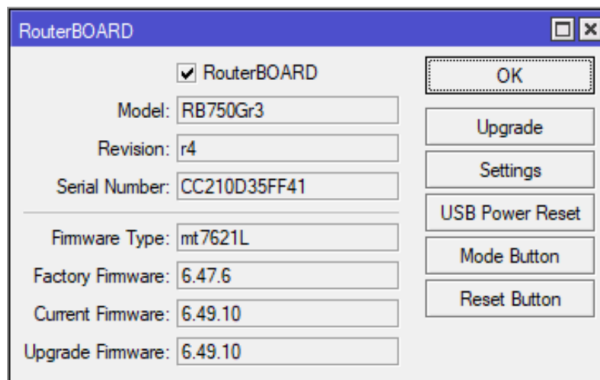
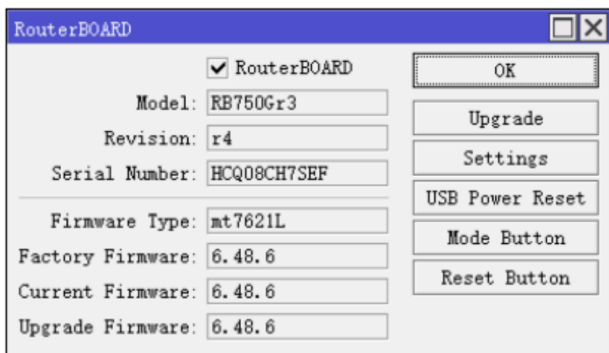
1	Introdução	3
2	Configuração do Roteador Mikrotik:	3
3	Configuração do Certificado:	3
3.1	Criar Certificado CA	3
3.2	Criar e assinar o Certificado do Servidor	4
3.3	Crie e assine o Certificado Client	5
3.4	Exporte o Certificado de autoridade (CA)	6
3.5	Exporte o Certificado Client	6
3.6	Baixe os certificados	7
4	IP Pool	7
4.1	Configure IP Pool	7
4.2	Configure Profile PPP	7
4.3	Crie um usuário	9
4.4	Ative o Servidor OpenVPN	9
5	Configuração do R3005G	10
5.1	Informações do dispositivo	10
5.2	Faça o Upload dos certificados	10
5.3	Checando o status da conexão	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

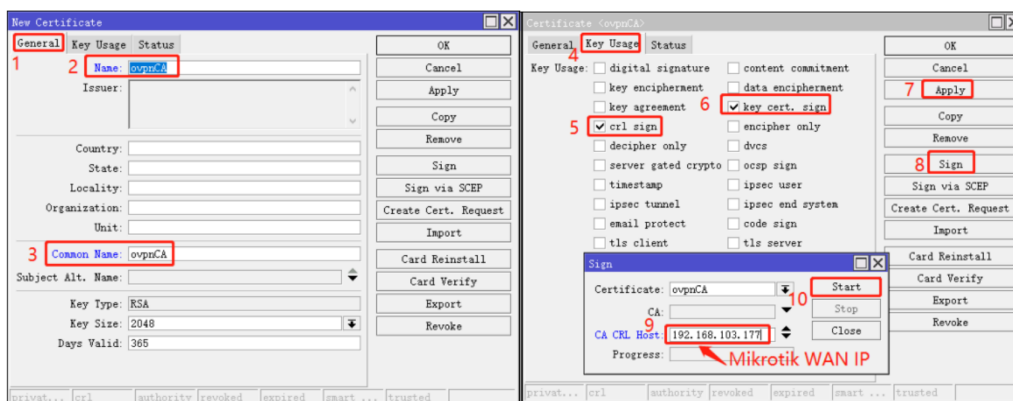


3 Configuração do Certificado:

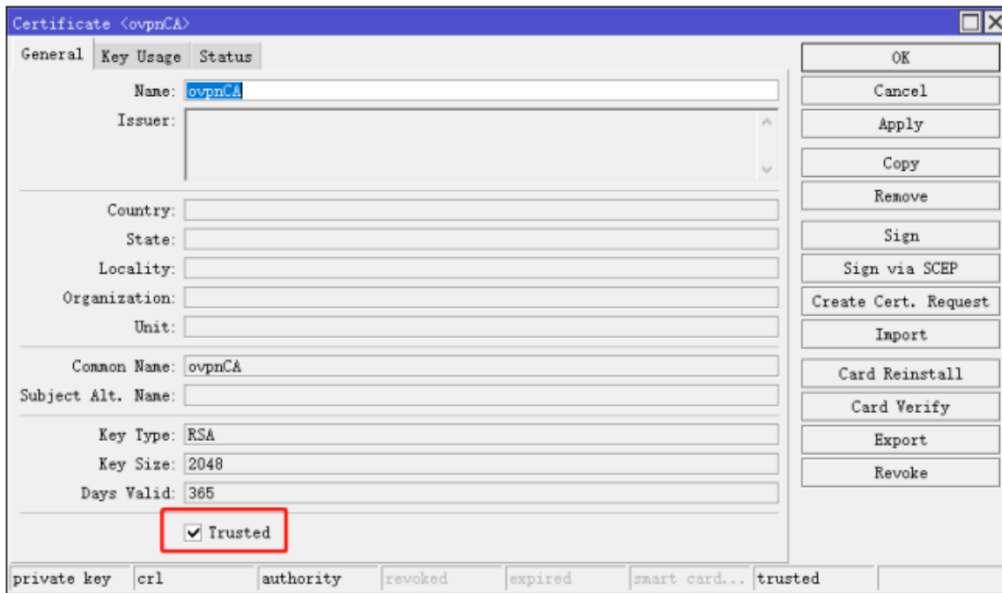
- Entre em System > Certificates > Certificates; Na Página de criação de certificados crie o CA, o certificado do Servidor e o certificado Client

3.1 Criar Certificado CA

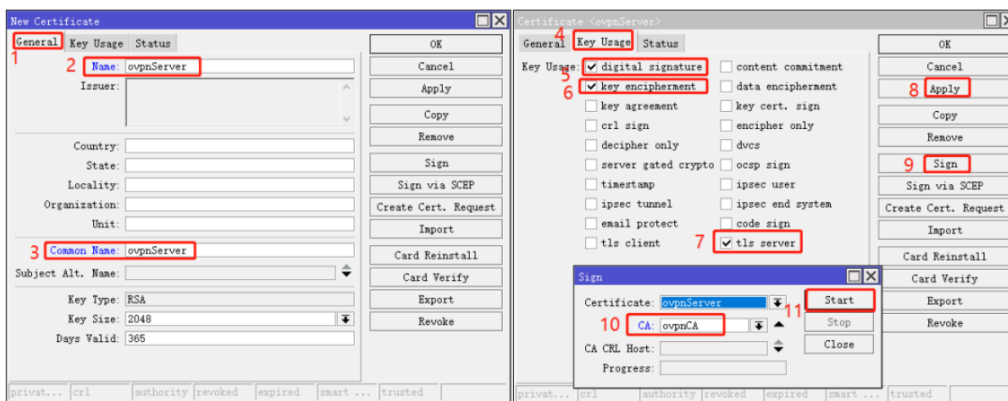
- Lembre-se de colocar o IP de Wan do mikrotik onde as requisições de OpenVPN irão chegar ao assinar o certificado, pois o mikrotik em versões mais antigas podem ter alguns problemas para negociar os certificados se não houver esta informação.



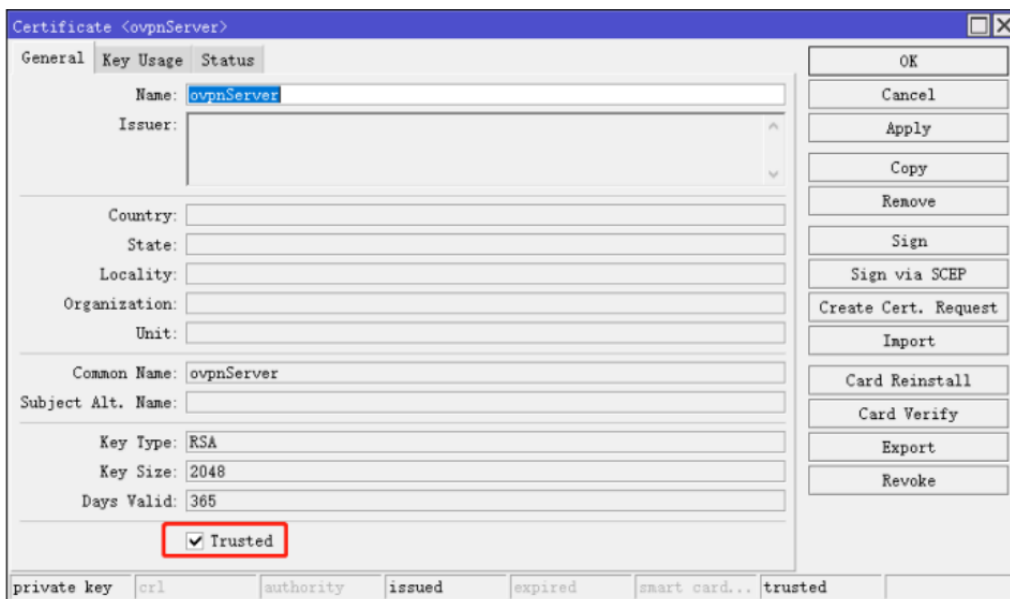
Confirme se o Checkbox "Trusted" está marcado conforme abaixo:



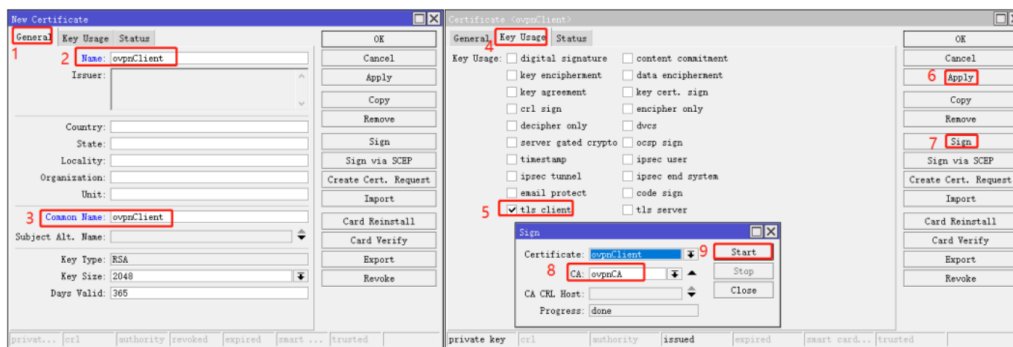
3.2 Criar e assinar o Certificado do Servidor



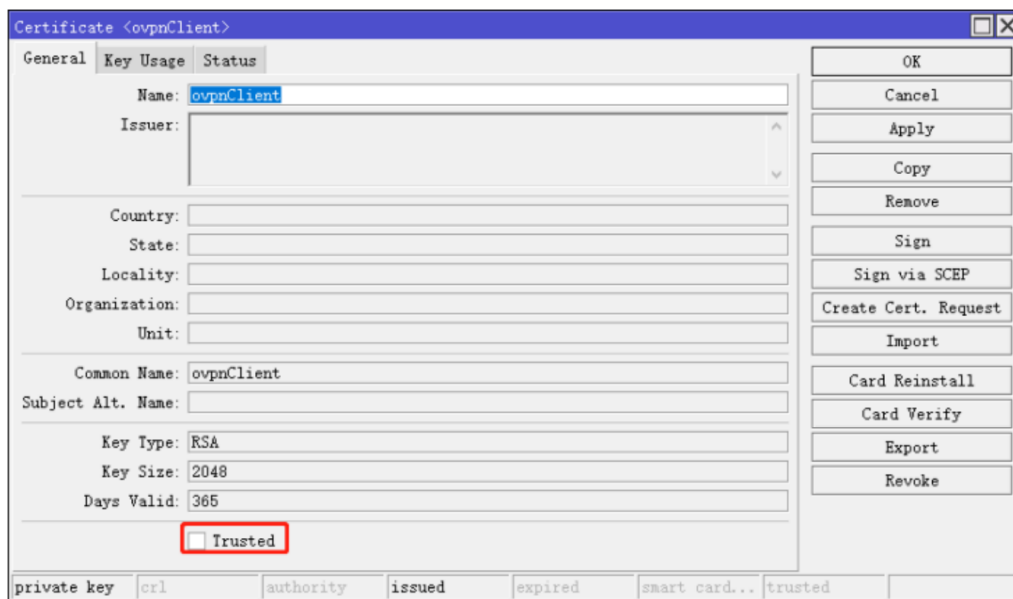
Confirme se o checkbox “Trusted” está marcado, conforme abaixo:



3.3 Crie e assine o Certificado Client



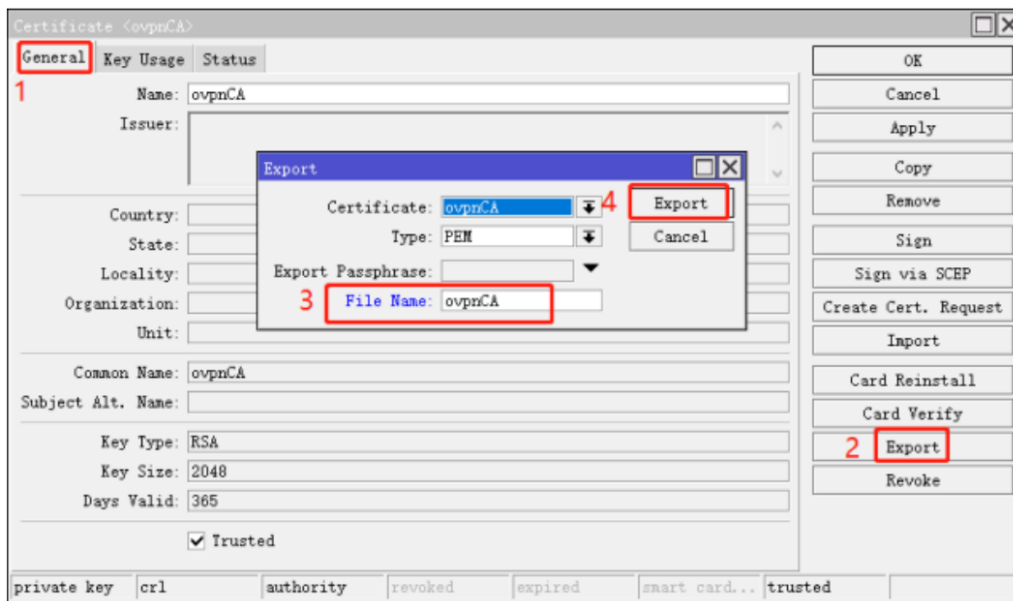
Neste caso o checkbox “Trusted” está desmarcado, conforme abaixo:



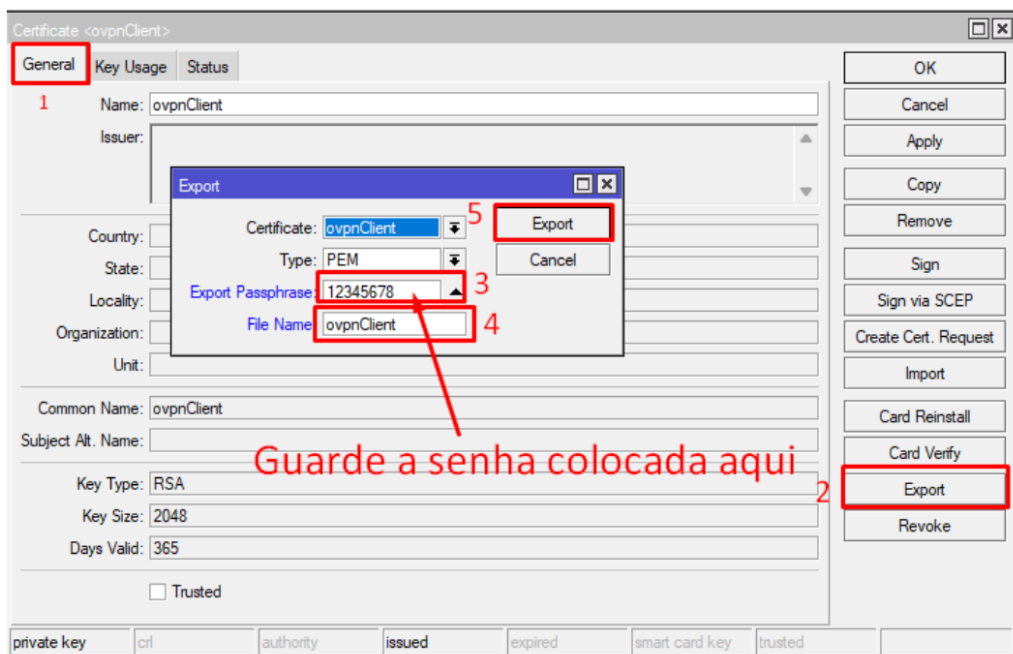
- Verifique se os 3 certificados foram criados corretamente

Certificates										
Certificates										
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	

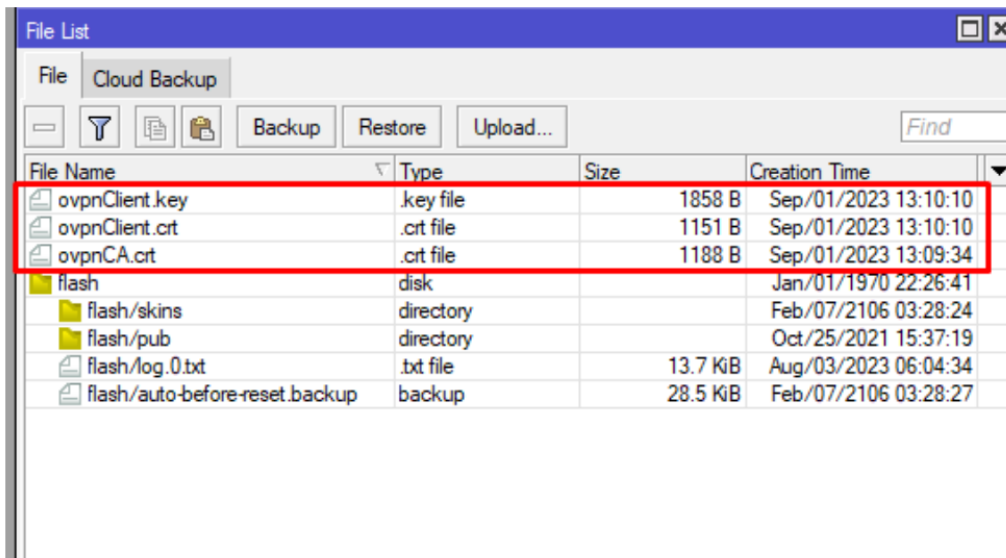
3.4 Exporte o Certificado de autoridade (CA)



3.5 Exporte o Certificado Client



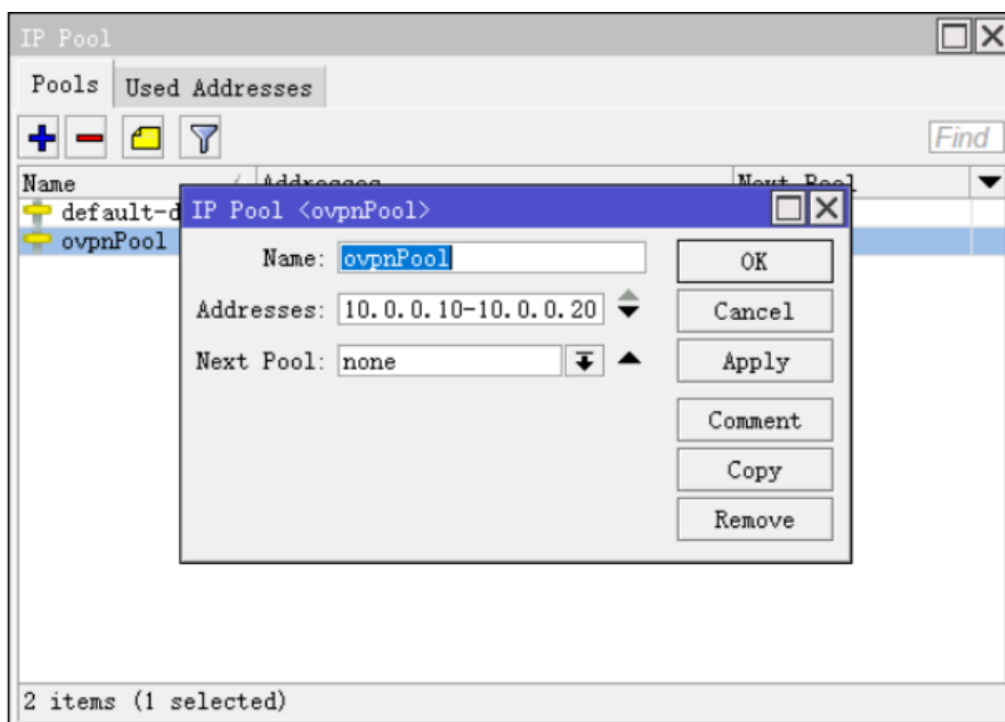
3.6 Baixe os certificados



4 IP Pool

4.1 Configure IP Pool

- IP > IP Pool > novo Pool



4.2 Configure Profile PPP

- PPP>Profiles

PPP Profile <ovpnProfile>

General Protocols Limits Queue Scripts

Name:

Local Address: [v] [▲]

Remote Address: [v] [▲]

Bridge: [v]

Bridge Port Priority: [v]

Bridge Path Cost: [v]

Bridge Horizon: [v]

Bridge Learning: [v]

Incoming Filter: [v]

Outgoing Filter: [v]

Address List: [▲▼]

Interface List: [v]

DNS Server: [▲▼]

[▲▼]

WINS Server: [▲▼]

- Change TCP MSS _____

no yes default

- Use UPnP _____

no yes default

OK

Cancel

Apply

Comment

Copy

Remove

4.3 Crie um usuário

The screenshot shows the 'PPP Secret <teste>' configuration window. The fields are filled with the following information:

- Name: teste
- Password: 12345678
- Service: ovpn
- Caller ID: (empty)
- Profile: ovpnProfile
- Local Address: (empty)
- Remote Address: (empty)
- Routes: (empty)
- Limit Bytes In: (empty)
- Limit Bytes Out: (empty)
- Last Logged Out: Sep/01/2023 14:50:20
- Last Caller ID: 10.100.26.167
- Last Disconnect Reason: hung up

At the bottom left, the status is 'enabled'. On the right side, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

4.4 Ative o Servidor OpenVPN

The screenshot shows the 'OpenVPN Server' configuration window. The window is titled 'OpenVPN Server' and has several fields and options:

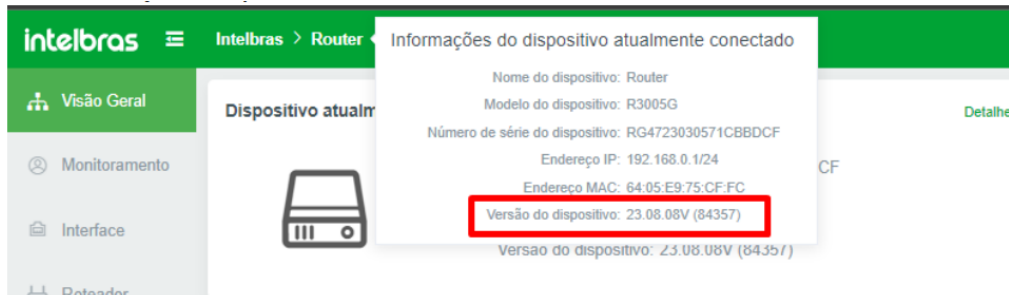
- 3**: Enabled
- Port: 4443
- Mode: tp
- Netmask: 24
- MAC Address: FE:50:C6:81:4A:31
- Max MTU: 1400
- Keepalive Timeout: 60
- Default Profile: ovpnProfile **4**
- Certificate: ovpnServer **5**
- 6**: Require Client Certificate
- Auth: sha1 md5
- Cipher: blowfish 128 aes 128 aes 256 **7** null

Numbered annotations (1-7) are present in the original image: 1 points to the 'Interface' tab, 2 to the 'OpenVPN Server' tab, 3 to the 'Enabled' checkbox, 4 to the 'Default Profile' dropdown, 5 to the 'Certificate' dropdown, 6 to the 'Require Client Certificate' checkbox, and 7 to the 'aes 256' cipher option.

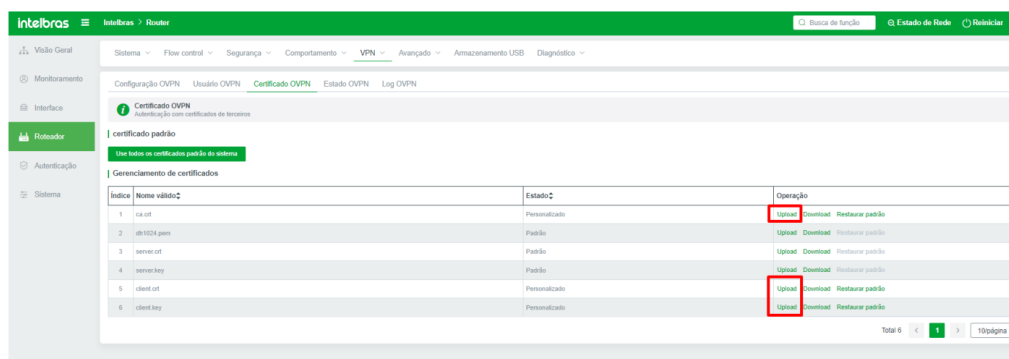
Feito isso, lembre-se de liberar no firewall para aceitar as requisições da porta 4443 ou a outra porta que for utilizar para o serviço

5 Configuração do R3005G

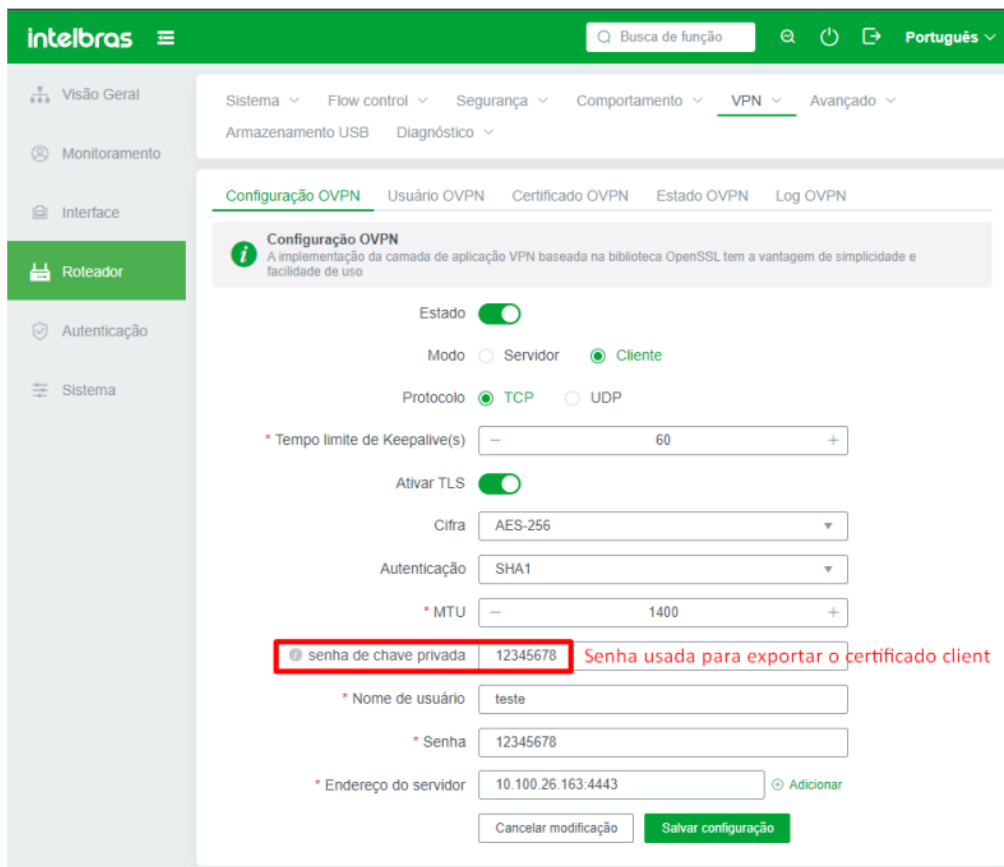
5.1 Informações do dispositivo



5.2 Faça o Upload dos certificados



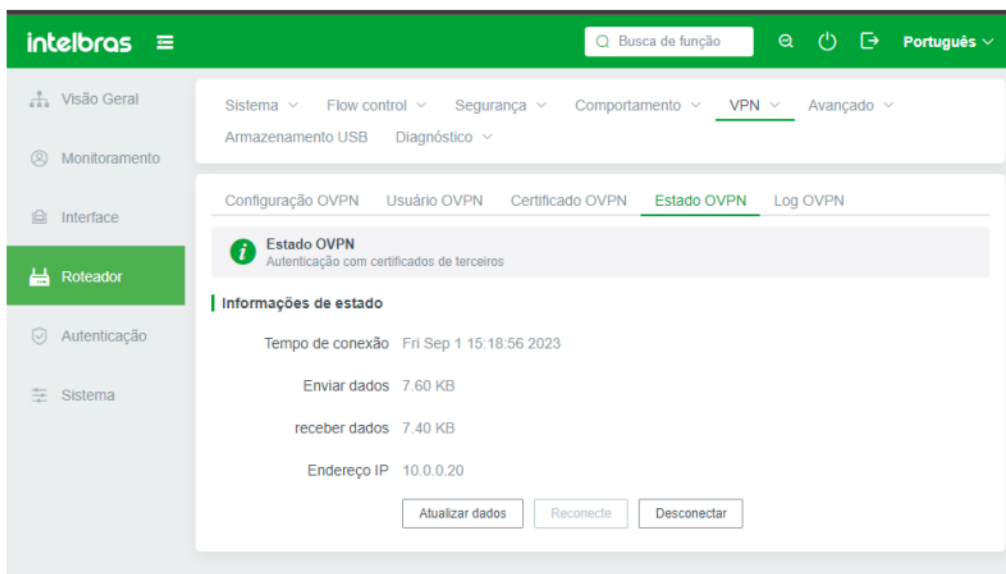
- Configure os parâmetros do cliente OpenVPN conforme o cenário configurado em seu servidor OpenVPN com o secret configurado, senha e o IP do mikrotik que irá receber as requisições.
- É muito importante que o IP seja o mesmo IP configurado no certificado de autoridade do mikrotik, pois se estiver divergente,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



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



- 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

#	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
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
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
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

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.

#	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 error: ssl: certificate not yet valid (6)>
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 error: ssl: certificate not yet valid (6)>
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	<ovpn-teste>: connected

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