

OVPN on RouterBoard

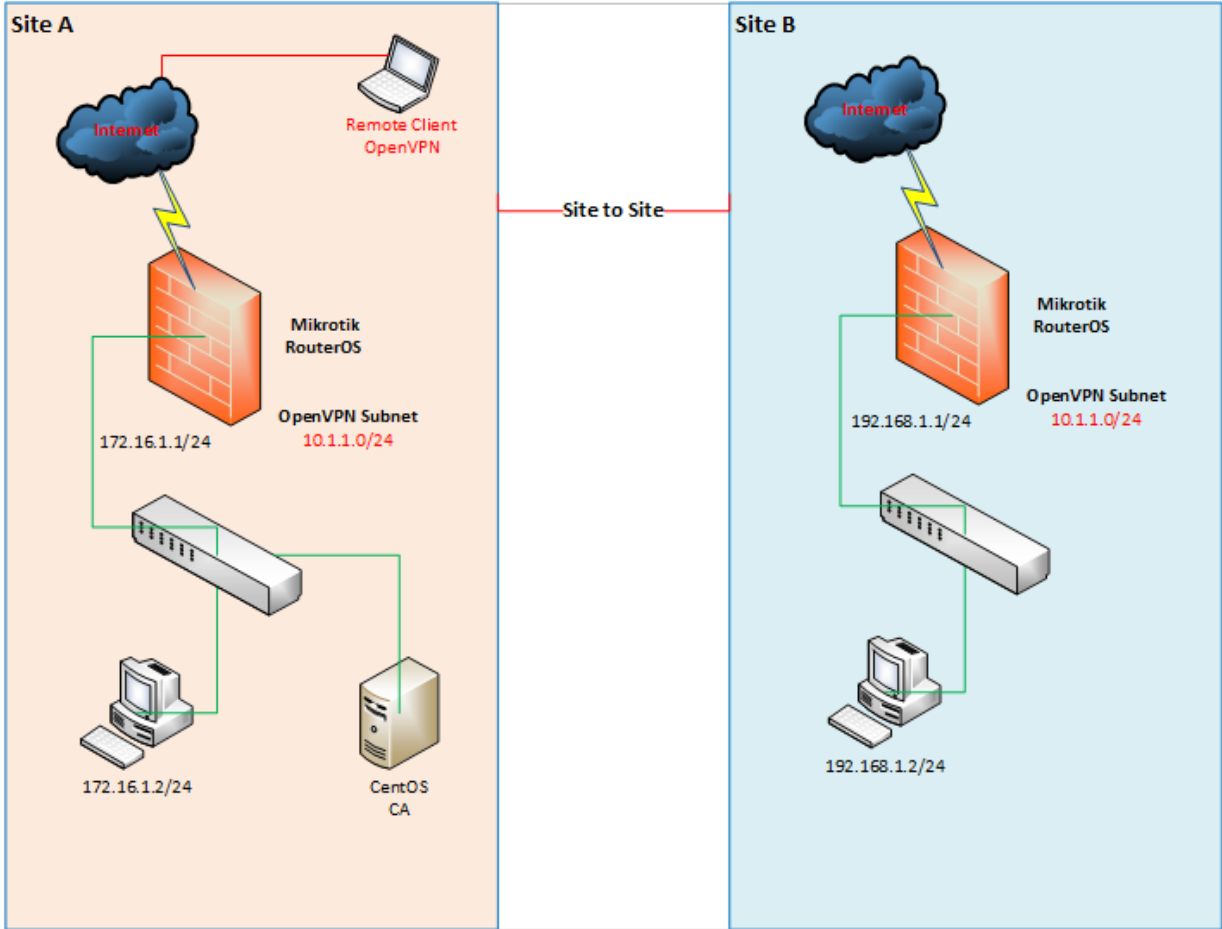
Site to Site

Client to Site

Who I am?

- Sun Sopheary
 - Email: sunsopheary@gmail.com
- IT Manager at Angkor Hospital for Children for more than 10 years
- RouterOS user since 2009
- MTCNA and MTCRE

Network Diagram



Different of Tunnels

Tunnel	Encryption	Protocol/Port	Notes
EoIP	None	IP no 47 (GRE)	<ul style="list-style-type: none">- Proprietary Mikrotik- Possible to be bridge
PPTP	MPPE 128 bit	TCP 1723	<ul style="list-style-type: none">- Most widely used- PPTP client can run almost in all OS
L2TP	Borrow IPSEC 168 bit	UDP 1701	<ul style="list-style-type: none">- Not has encryption so borrow IPsec- But not mandatory using IPsec
SSTP	SSL 2048 bit	TCP 443	<ul style="list-style-type: none">- Usually never block by firewall- Very secure
PPPOE	MPPE 128 bit	Frame	<ul style="list-style-type: none">- Layer 2 tunnel- Cannot pass the router
OpenVPN	SSL	TCP 443, TCP 1194 (RB)	<ul style="list-style-type: none">- Usually never block by firewall- Very secure

Why to use OpenVPN

- It has been ported to various platforms, including Linux and Windows.
- It's configuration is throughout likewise on each of these systems, so it makes it easier to support and maintain.

OVPN Features of RouterOS

- Supported
 - TCP
 - Bridging (tap device)
 - Routing (tun device)
 - Certificate
- Unsupported
 - UDP
 - LZO compression

Routed vs Bridging VPN

- Overall, routing is probably a better choice for most people, as it is more efficient and easier to set up (as far as the OpenVPN configuration itself) than bridging.
- Routing also provides a greater ability to selectively control access rights on a client-specific basis.
- Routing is commended unless you need a specific feature which requires bridging, such as:
 - The VPN needs to be able to handle non-IP protocols such as IPX,
 - You are running applications over the VPN which rely on network broadcasts (such as LAN games)
 - You would like to allow browsing of Windows file shares across the VPN without setting up a Samba or WINS server.

Step to configure OVPN

1. Generate CA certificate (Assumed KPI is already exist).
2. Generate a server certificate for RB at Site A.
3. Generate two certificates for OpenVPN clients, one certificate for RB at Site B and another one for a remote client laptop.
4. Import [CA and server certificate](#) for RB at Site A. Configure OpenVPN server on RB at Site A.
5. Import [CA and client certificate](#) for RB at Site B. Configure OpenVPN client on RB at Site B.
6. Verify the connection and configuration for both sites.
7. Configure OpenVPN client on a remote laptop and make a connection.

Step 1: Generate CA certificate

- Edit parameters inside vars file under the directory EasyRSA
 - `root@ca EasyRSA# vi vars`

```
export KEY_COUNTRY="KH"  
export KEY_PROVINCE="SR"  
export KEY_CITY="Siem Reap"  
export KEY_ORG="Angkor Hospital for Children"  
export KEY_EMAIL="sunsopheary@angkorhospital.org"  
export KEY_OU="IT Unit"
```

- Then, choose a system to act as your CA and create a new PKI and CA:
 - `root@ca EasyRSA# ./easysrsa init-pki`
 - `root@ca EasyRSA# ./easysrsa build-ca`
- `ca.crt` and `ca.key` file will be built.

Step 2: Generate a certificate for RB at Site A.

- root@ca EasyRSA# ./easyrsa build-server-full siteA-rb

```
[root@ca EasyRSA-3.0.0-rc2]# ./easyrsa build-server-full siteA-rb

Note: using Easy-RSA configuration from: ./vars
Generating a 4096 bit RSA private key
.....
..++
...++
writing new private key to '/root/EasyRSA-3.0.0-rc2/pki/private/siteA-rb.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----

Using configuration from /root/EasyRSA-3.0.0-rc2/openssl-1.0.cnf
Enter pass phrase for /root/EasyRSA-3.0.0-rc2/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName          :PRINTABLE:'siteA-rb'
Certificate is to be certified until Jan 11 04:17:31 2027 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
[root@ca EasyRSA-3.0.0-rc2]#
```

Step 3: Generate a client certificate for RB at Site B.

- root@ca EasyRSA# ./easymrsa build-client-full siteB-rb

```
[root@ca EasyRSA-3.0.0-rc2]# ./easymrsa build-client-full siteB-rb

Note: using Easy-RSA configuration from: ./vars
Generating a 4096 bit RSA private key
.....++
.....++
writing new private key to '/root/EasyRSA-3.0.0-rc2/pki/private/siteB-rb.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /root/EasyRSA-3.0.0-rc2/openssl-1.0.cnf
Enter pass phrase for /root/EasyRSA-3.0.0-rc2/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName          :PRINTABLE:'siteB-rb'
Certificate is to be certified until Jan 11 04:24:11 2027 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
[root@ca EasyRSA-3.0.0-rc2]#
```

Step 3: Generate a client certificate for a remote laptop

- root@ca EasyRSA# ./ easyrsa build-client-full pheary-laptop

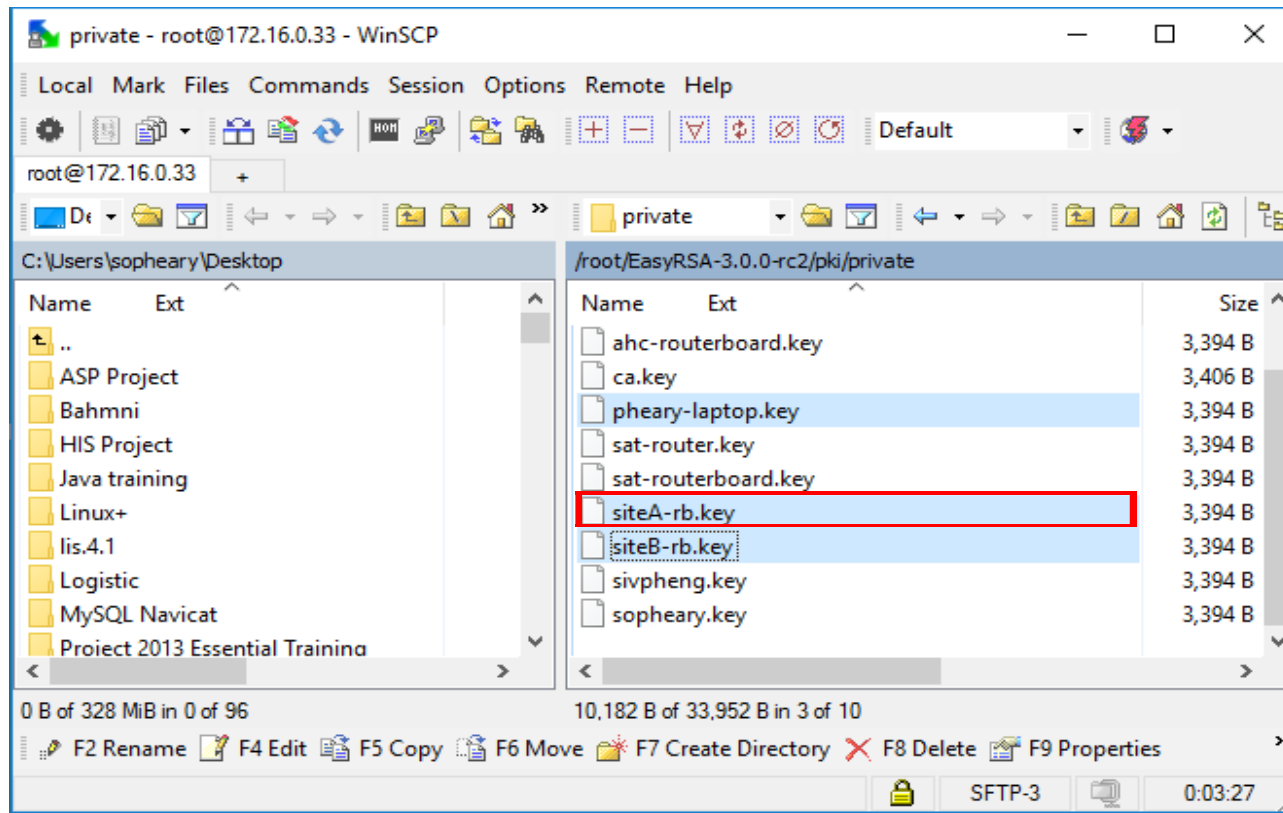
```
[root@ca EasyRSA-3.0.0-rc2]# ./easyrsa build-client-full pheary-laptop

Note: using Easy-RSA configuration from: ./vars
Generating a 4096 bit RSA private key
.....
.....
.....++
writing new private key to '/root/EasyRSA-3.0.0-rc2/pki/private/pheary-laptop.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /root/EasyRSA-3.0.0-rc2/openssl-1.0.cnf
Enter pass phrase for /root/EasyRSA-3.0.0-rc2/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :PRINTABLE:'pheary-laptop'
Certificate is to be certified until Jan 11 04:29:42 2027 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
[root@ca EasyRSA-3.0.0-rc2]#
```

Step 4: Import CA and server certificate for RB at Site A

- Use WinSCP to copy below certificates from CA machine.
 - ca.crt (path: /root/EasyRSA-3.0.0-rc2/pki)
 - siteA-rb.key (path: /root/EasyRSA-3.0.0-rc2/pki/private)
 - siteA-rb.crt (path: /root/EasyRSA-3.0.0-rc2/pki/issued)



Step 4: Import CA and server certificate for RB at Site A (Cont...)

- Upload certificates to RB

File Name	Type	Size	Creation Time
	script	57.6 KB	Dec/16/2016 10:41:32
	script	57.1 KB	Oct/21/2016 15:18:21
17.backup	backup	266.0 KB	Oct/21/2016 15:17:42
40.backup	backup	267.5 KB	Dec/16/2016 10:40:56
	.txt file	54.5 KB	Jan/13/2017 13:26:23
	.txt file	172.1 KB	Jan/13/2017 11:12:53
	.crt file	6.9 KB	Aug/18/2015 16:06:17
	.key file	3394 B	Aug/18/2015 16:06:17
ca.crt	.crt file	1834 B	Aug/18/2015 16:06:17
log.0.txt	.txt file	1883 B	Dec/31/2016 14:19:42
log.1.txt	.txt file	62.0 KB	Dec/23/2016 09:21:22
pub	directory		Jan/02/1970 07:12:32
siteA-rb.crt	.crt file	6.9 KB	Jan/13/2017 13:26:17
siteA-rb.key	.key file	3394 B	Jan/13/2017 13:26:17
skins	directory		Jan/01/1970 07:00:03
sys-note.txt	.txt file	65 B	Oct/22/2016 12:58:39
web-proxy1	web-proxy store		May/01/2016 09:41:43

Step 4: Import CA and server certificate for RB at Site A (Cont...)

- Import certificates (system->Certificate->import)

The screenshots illustrate the process of importing certificates into the Windows Certificate Manager console. Each screenshot shows the 'Certificates' console with the 'Import' dialog box open. Red circles with numbers 1 through 4 highlight the key actions in each step.

Step 1: The 'Import' dialog box shows 'Only File: ca.crt' and 'Passphrase: *****'. The 'Import' button is highlighted.

Step 2: The 'Import' dialog box shows 'Only File: siteA-rb.crt' and 'Passphrase: *****'. The 'Import' button is highlighted.

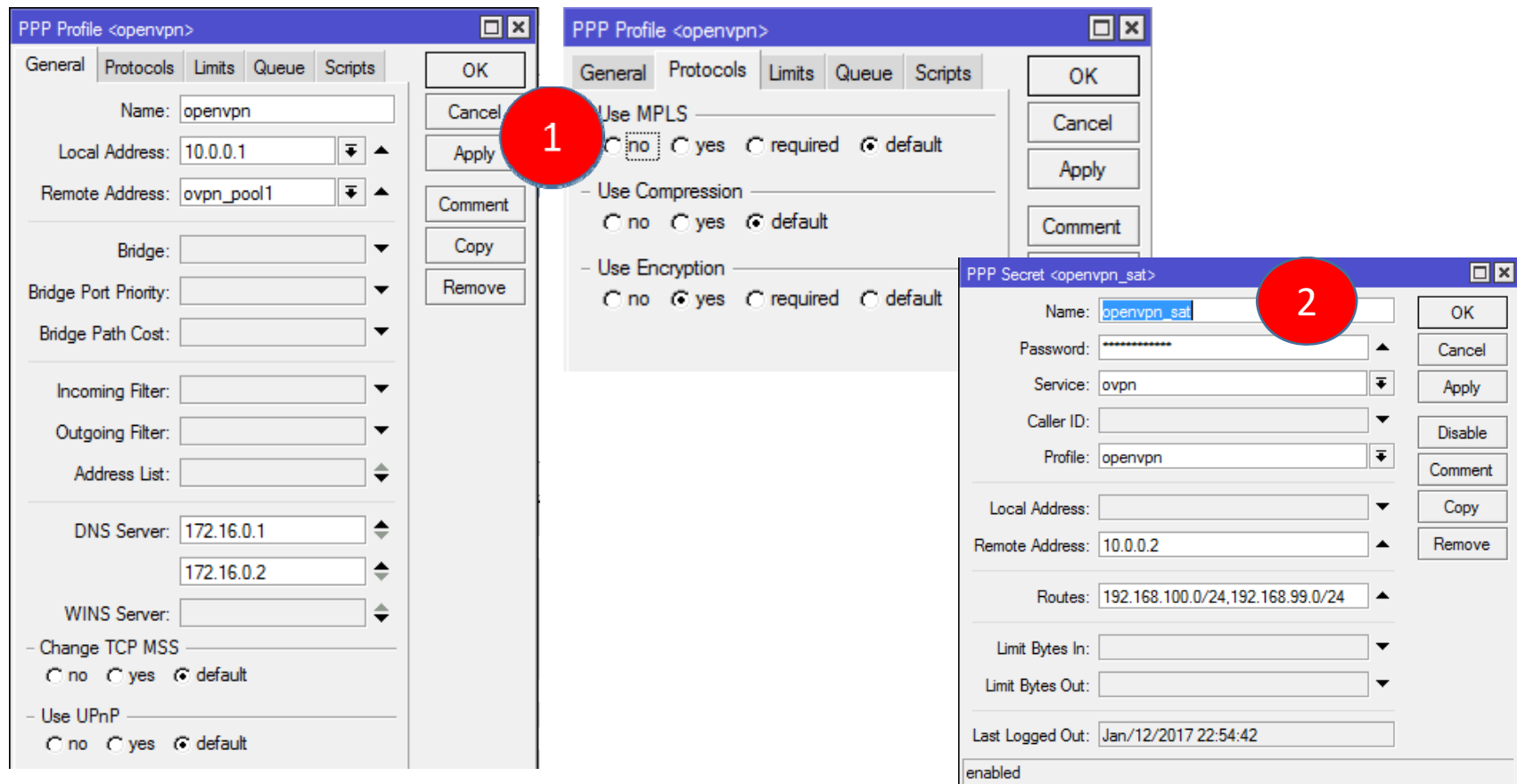
Step 3: The 'Import' dialog box shows 'Only File: siteA-rb.key' and 'Passphrase: *****'. The 'Import' button is highlighted.

Step 4: The 'Certificates' console displays a table of imported certificates. The table is highlighted with a red border.

	Name	Issuer	Common Name	Subject
T	myca	CN=myca	myca	::
KT	siteA-rb	CN=myca	siteA-rb	::

Step 4: Configure OVPN server on RB at Site A (Cont...)

1. Configure profile (PPP -> Profiles)
2. Configure secret (PPP -> Secrets)



Step 4: Configure OVPN server on RB at Site A (Cont...)

- Enable OVPN Server (PPP -> Interface -> OVPN Server)

OVPN Server

Enabled

Port: 1194

Mode: ip

Netmask: 24

MAC Address: FE:38:47:E3:04:52

Max MTU: 1500

Keepalive Timeout: 60

Default Profile: openvpn

Certificate: siteA-rb

Require Client Certificate

Auth.: sha1 md5
 null

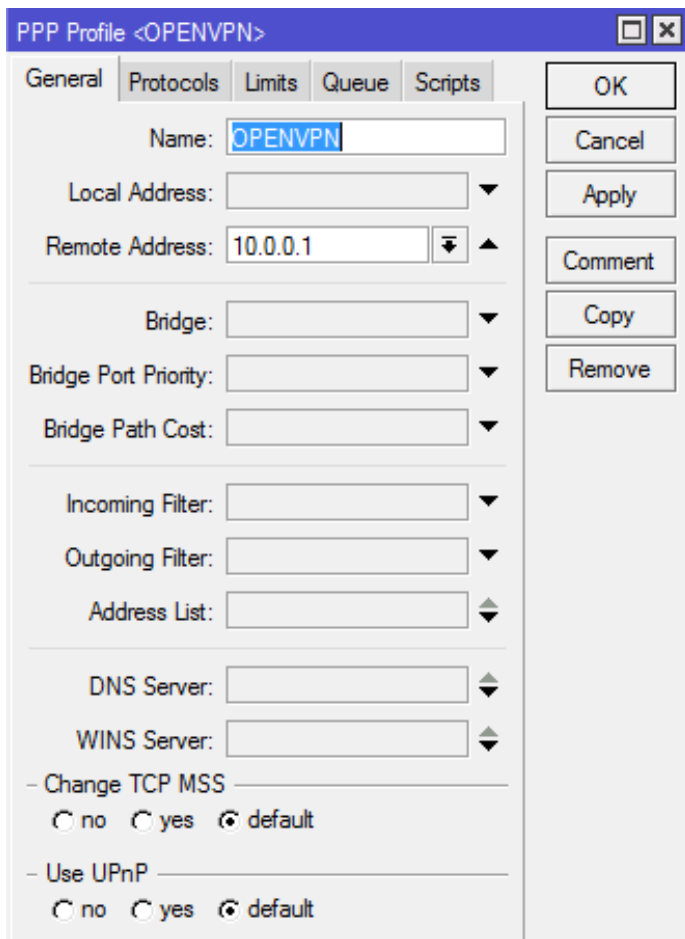
Cipher: blowfish 128 aes 128
 aes 192 aes 256
 null

OK
Cancel
Apply

- Note: Make sure port 1194 is opened on RB at Site A for input chain.

Step 5: Import CA, client certificate, and configure client profile on RB at Site B

- Upload and import certificates to RB.
- Configure profile (PPP -> Profiles)



PPP Profile <OPENVPN>

General Protocols Limits Queue Scripts

Name: OPENVPN

Local Address: []

Remote Address: 10.0.0.1

Bridge: []

Bridge Port Priority: []

Bridge Path Cost: []

Incoming Filter: []

Outgoing Filter: []

Address List: []

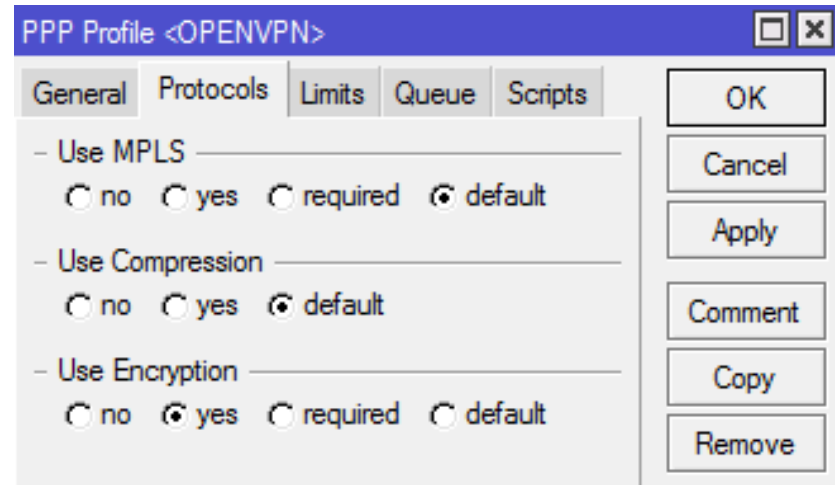
DNS Server: []

WINS Server: []

- Change TCP MSS ————
 no yes default

- Use UPnP ————
 no yes default

OK Cancel Apply Comment Copy Remove



PPP Profile <OPENVPN>

General Protocols Limits Queue Scripts

- Use MPLS ————
 no yes required default

- Use Compression ————
 no yes default

- Use Encryption ————
 no yes required default

OK Cancel Apply Comment Copy Remove

Step 5: Configure OVPN client on RB at Site B

- Add interface for OVPN client (PPP -> Interface -> OVPN Client)

The image shows a sequence of three screenshots from the Mikrotik WinBox interface, illustrating the steps to configure an OVPN client interface.

Step 1: The first screenshot shows the 'PPP' menu. The 'OVPN Client' option is highlighted, and a red circle with the number '1' is placed over it.

Step 2: The second screenshot shows the 'Interface <ovpn-out-AHC-RB>' configuration window. The 'General' tab is selected, and the 'Type' is set to 'OVPN Client'. A red circle with the number '2' is placed over the 'Type' field.

Step 3: The third screenshot shows the 'Interface <ovpn-out-AHC-RB>' configuration window with the 'Dial Out' tab selected. The 'Connect To' field is set to '203.189...'. A red circle with the number '3' is placed over the 'Connect To' field.

Step 6: Verify the connection and configuration for both sites.

- Show the configuration on the real network at my place.
 - Double check the configuration for both RB on both sites
 - Check the active connection status
 - Check the routing table

Step 7: Configure OpenVPN client on a remote laptop

- Install OpenVPN for windows
- Demo the configuration
- Make connection to OVPN server on RB at Site A

Reference

- http://wiki.mikrotik.com/wiki/OpenVPN#Why_to_use_OpenVPN_.3F (Accessed on Jan 13th, 2017)
- <https://openvpn.net/index.php/open-source/documentation/howto.html#quick> (Accessed on Jan 13th, 2017)

Thank you!
Q & A