OVPN on RouterBoard

Site to Site

Client to Site

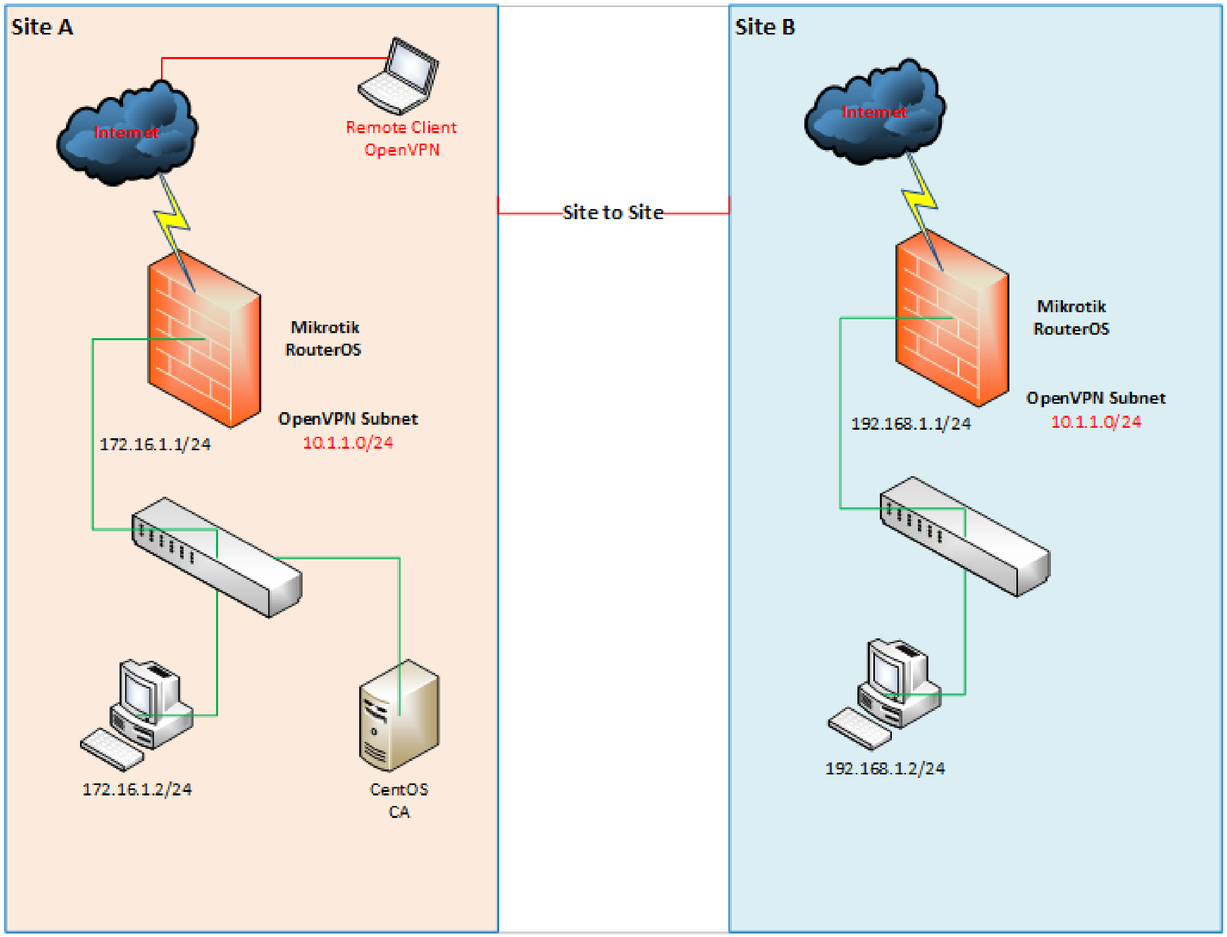
4/28/2017

Prepared by: Sun Sopheary

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)	- Proprietary Mikrotik - Possible to be bridge
PPTP	MPPE 128 bit	TCP 1723	- Most widely used - PPTP client can run almost in all OS
L2TP	Borrow IPSEC 168 bit	UDP 1701	- Not has encryption so borrow IPSec - But not mandatory using IPSec
SSTP	SSL 2048 bit	TCP 443	- Usually never block by firewall - Very secure
PPPOE	MPPE 128 bit	Frame	- Layer 2 tunnel - Cannot pass the router
OpenVPN	SSL	TCP 443, TCP 1194 (RB)	- 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

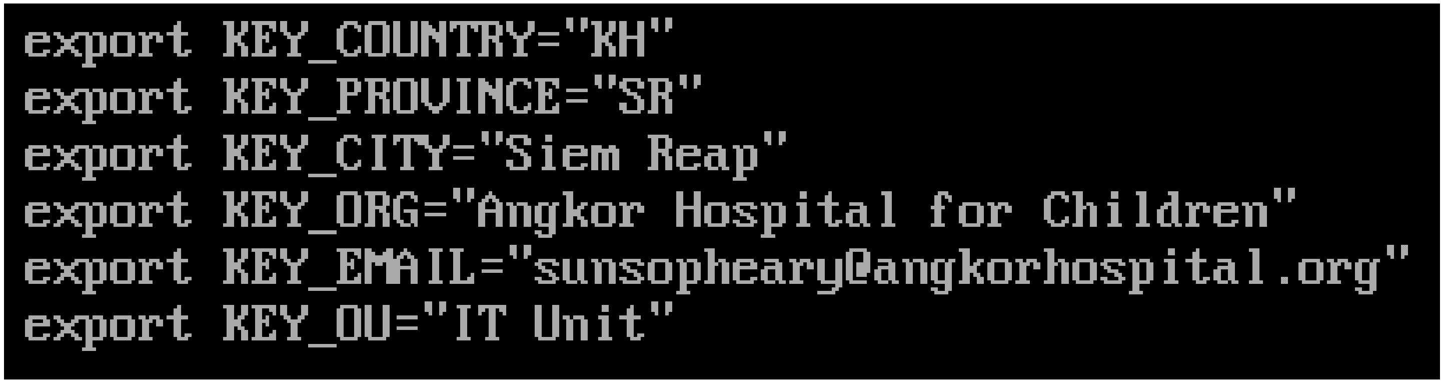
- Overall, routing is probably a better choice for most people, as it is more efficient and easier to set up (as far as the OpenVPN configuration itself) than bridging.
- Routing also provides a greater ability to selectively control access rights on a client-specific basis.
- Routing is commended unless 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



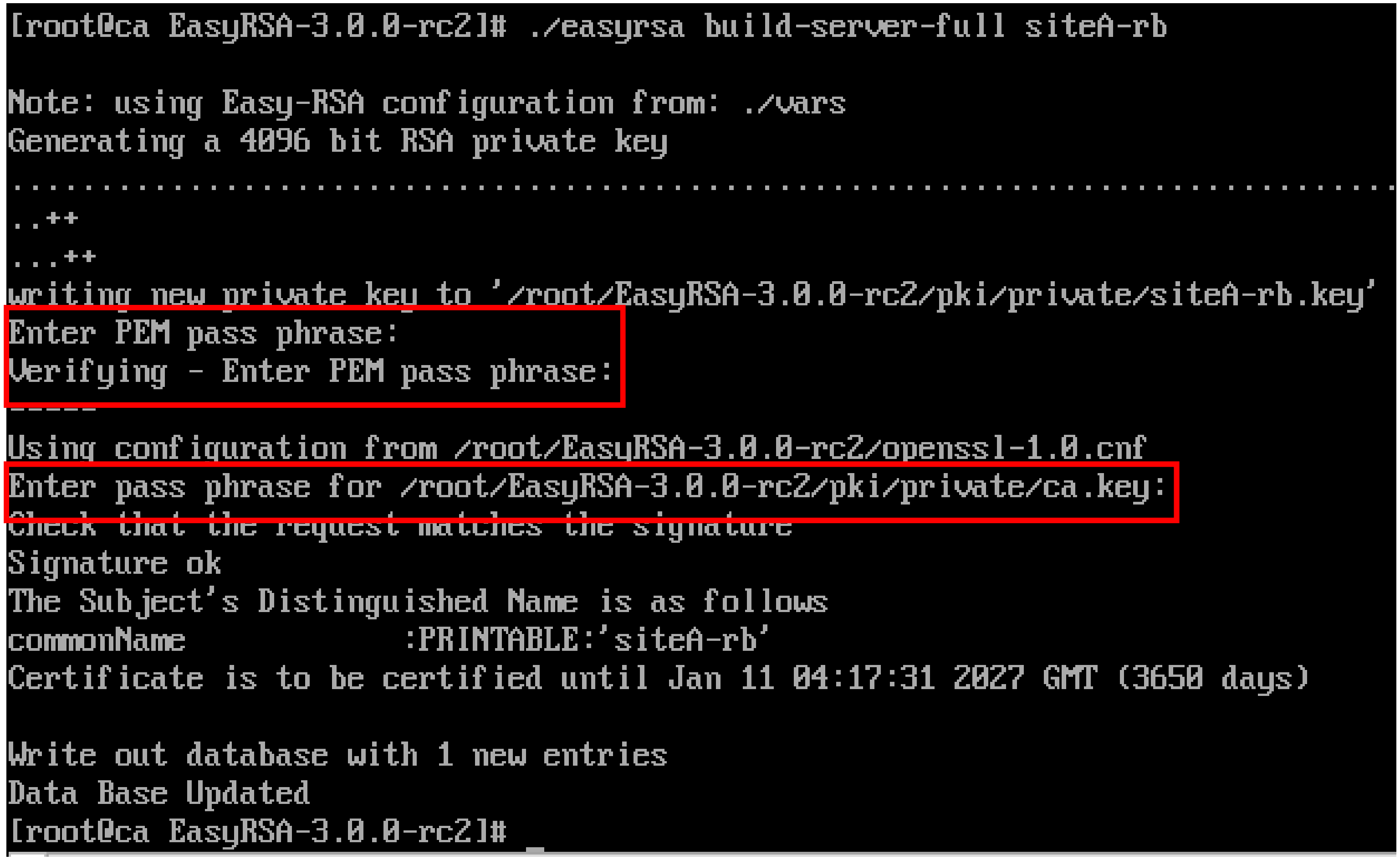
```
export KEY_COUNTRY="KH"
export KEY_PROVINCE="SR"
export KEY_CITY="Siem Reap"
export KEY_ORG="Angkor Hospital for Children"
export KEY_EMAIL="sunsopheary@angkorhospital.org"
export KEY_OU="IT Unit"
```

- Then, choose a system to act as your CA and create a new PKI and CA:
  - root@ca EasyRSA# ./easyrsa init-pki
  - root@ca EasyRSA# ./easyrsa 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



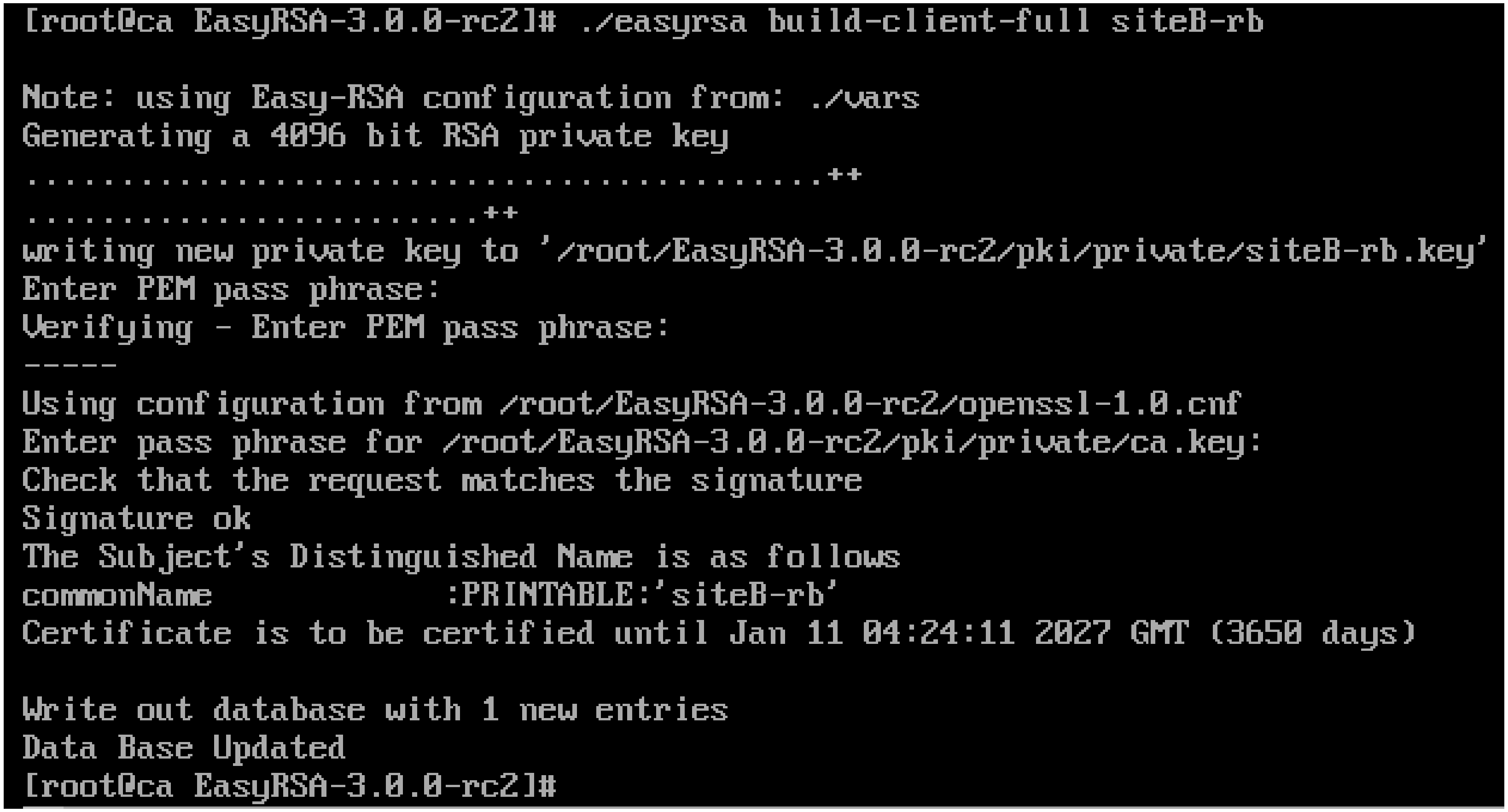
```
[root@ca EasyRSA-3.0.0-rc2]# ./easyrsa build-server-full siteA-rb

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# ./easyrsa build-client-full siteB-rb



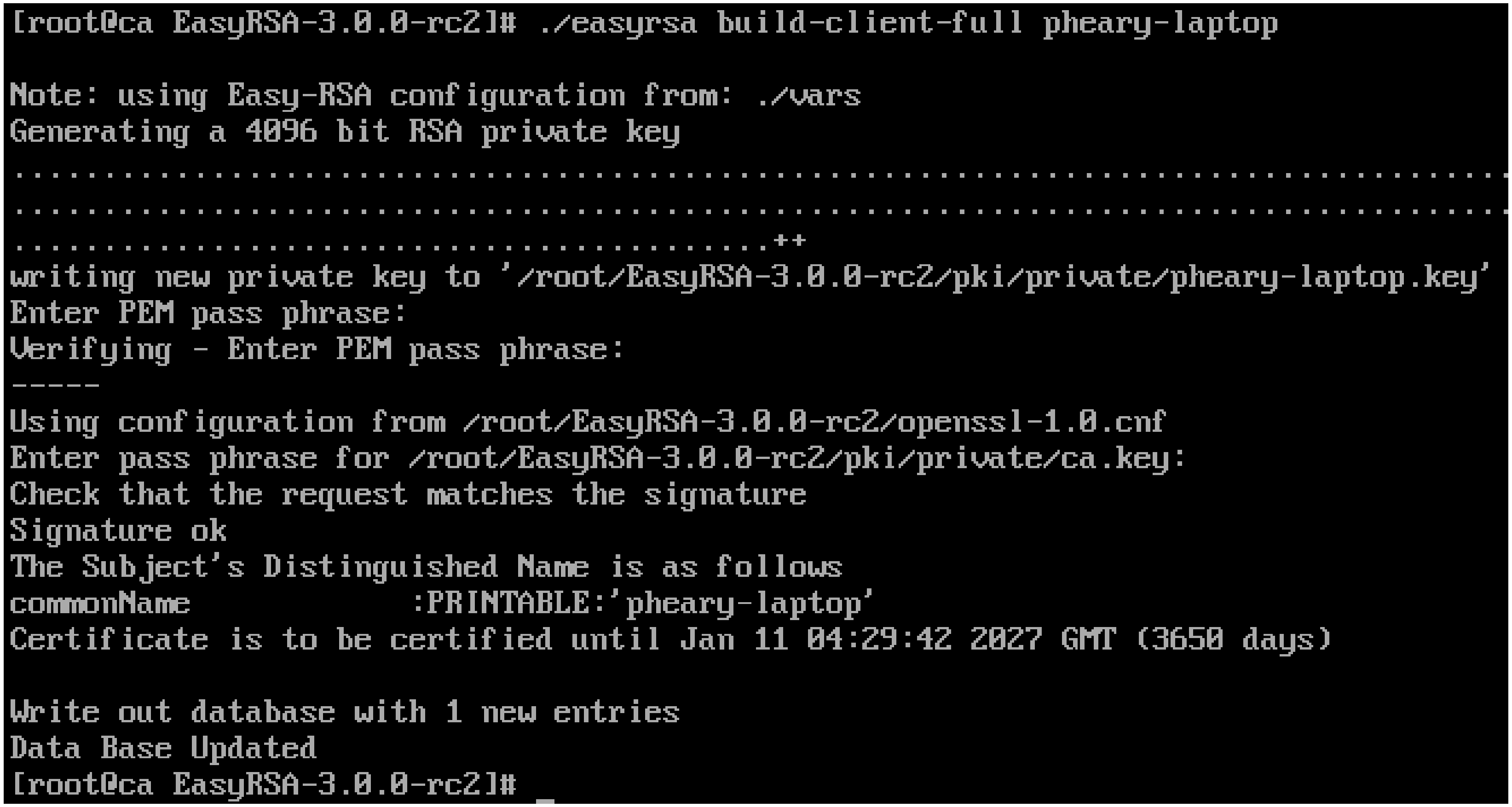
```
[root@ca EasyRSA-3.0.0-rc2]# ./easyrsa build-client-full siteB-rb

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



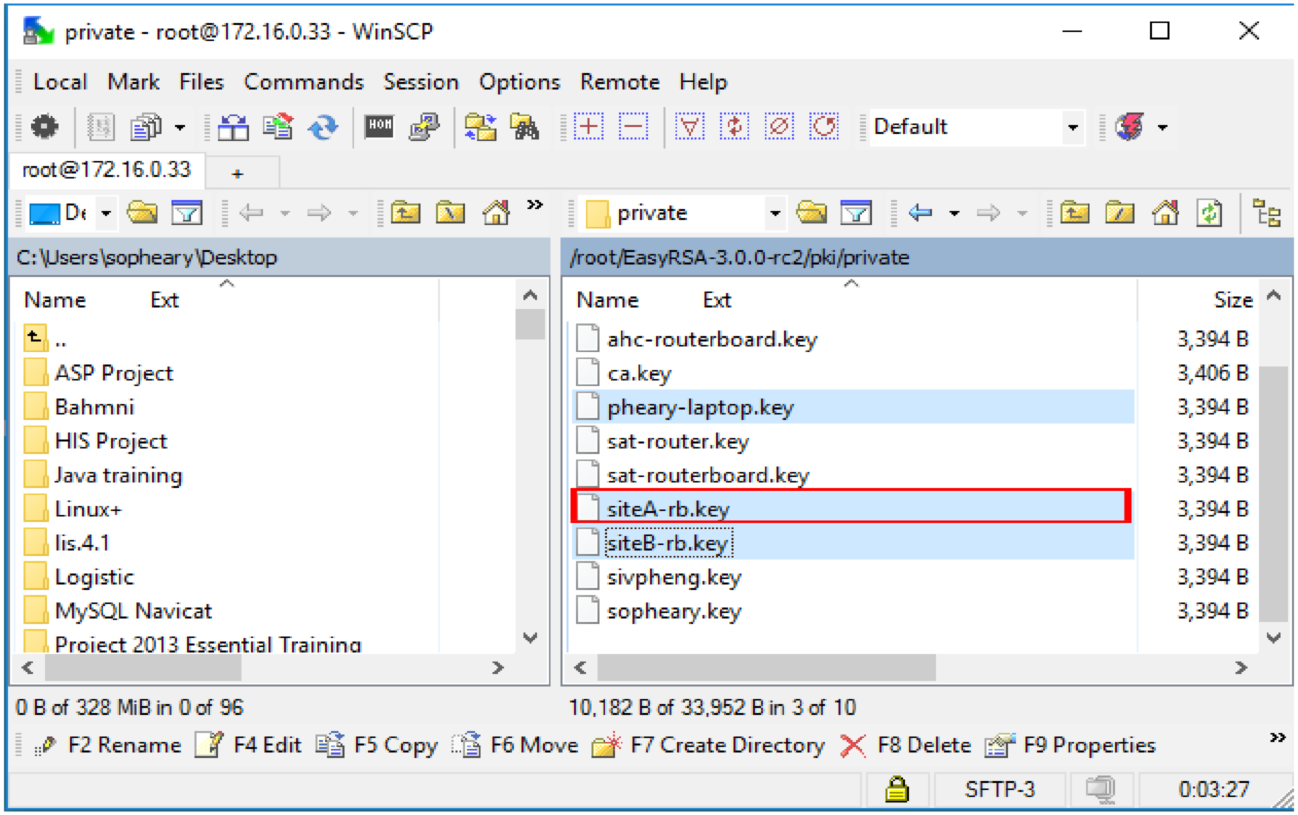
```
[root@ca EasyRSA-3.0.0-rc2]# ./easyrsa build-client-full pheary-laptop

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)



private - root@172.16.0.33 - WinSCP

C:\Users\sopheary\Desktop

Name	Ext
..	
ASP Project	
Bahmni	
HIS Project	
Java training	
Linux+	
lis.4.1	
Logistic	
MySQL Navicat	
Project 2013 Essential Training	

/root/EasyRSA-3.0.0-rc2/pki/private

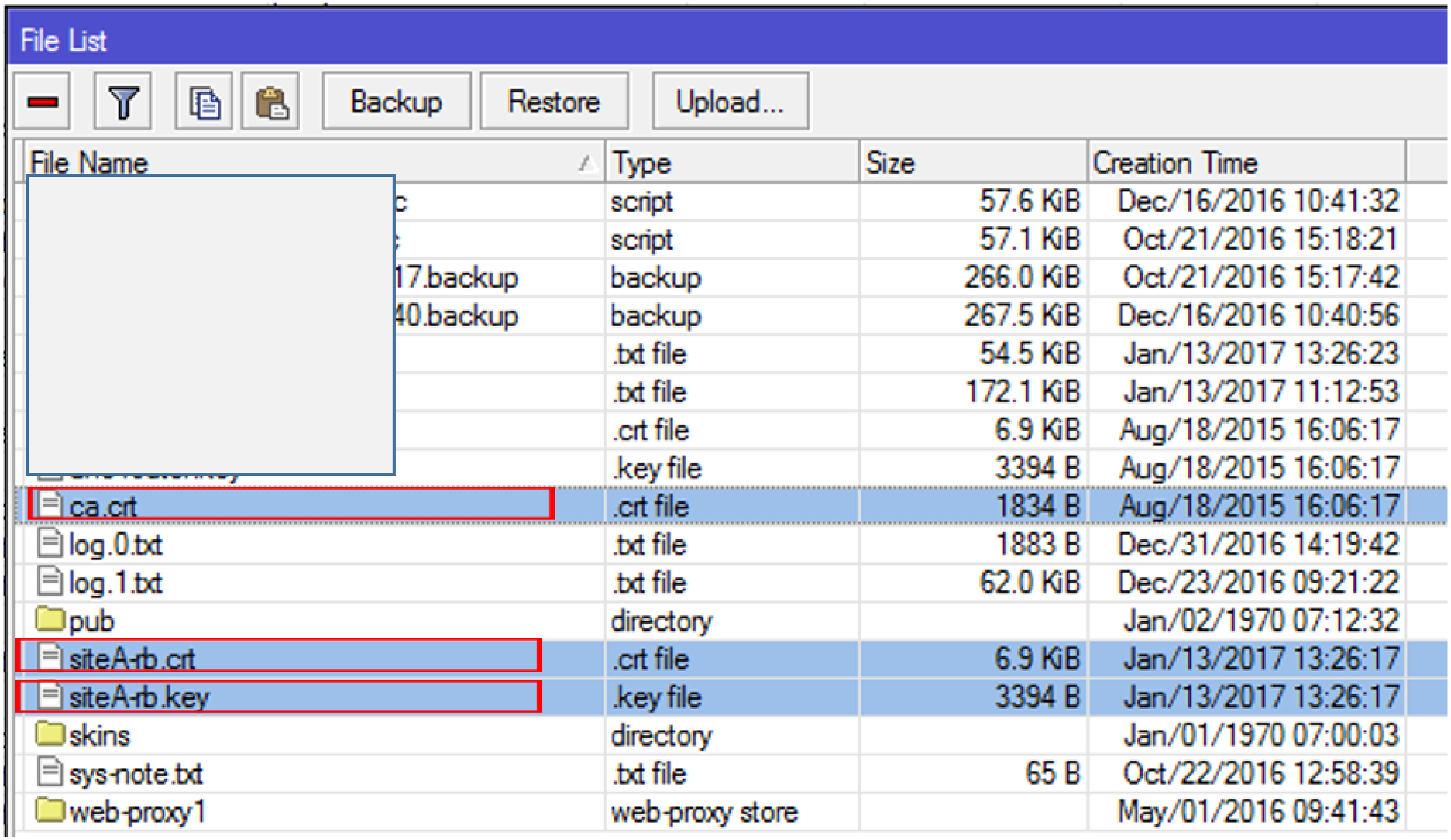
Name	Ext	Size
ahc-routerboard.key		3,394 B
ca.key		3,406 B
pheary-laptop.key		3,394 B
sat-router.key		3,394 B
sat-routerboard.key		3,394 B
siteA-rb.key		3,394 B
siteB-rb.key		3,394 B
sivpheng.key		3,394 B
sopheary.key		3,394 B

0 B of 328 MiB in 0 of 96

10,182 B of 33,952 B in 3 of 10

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

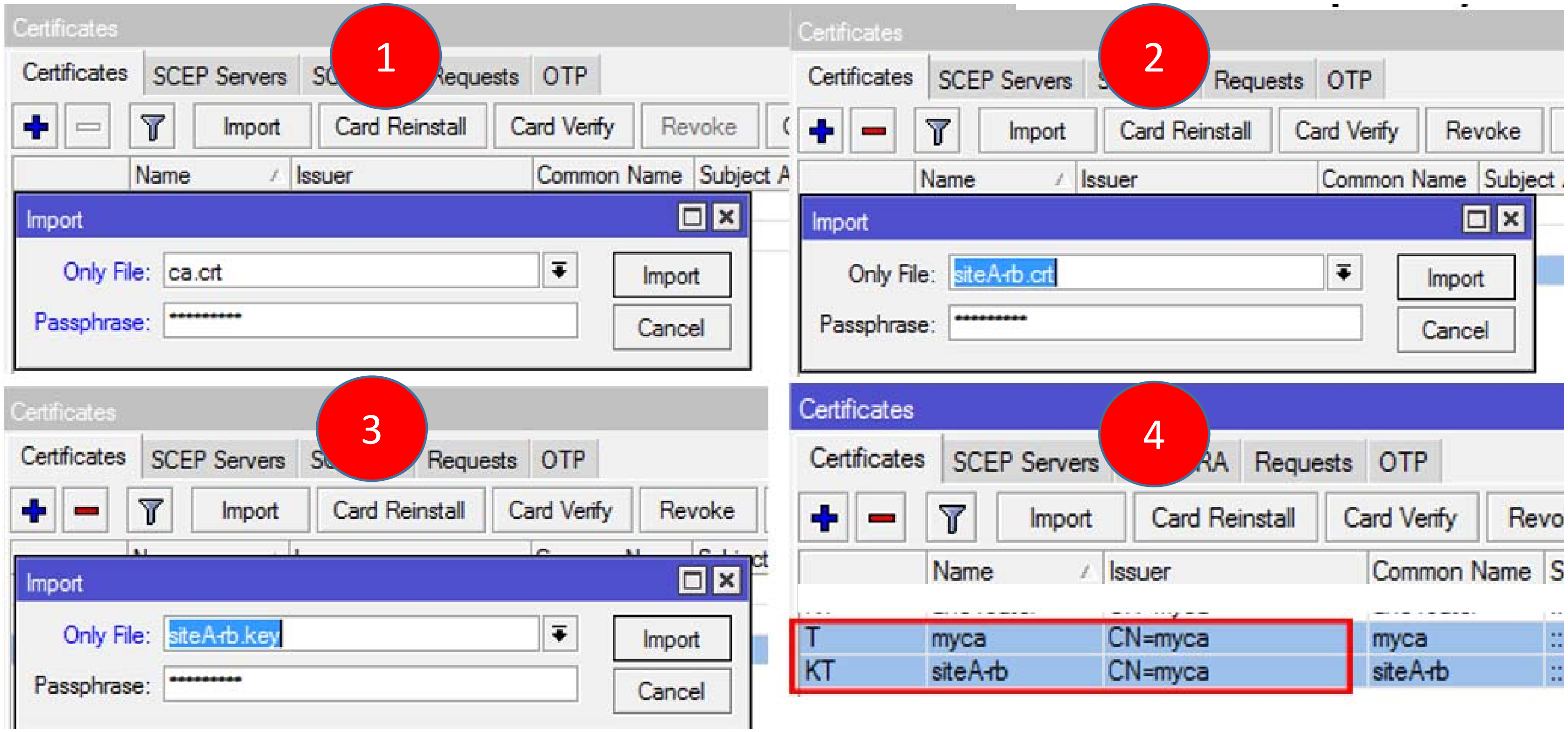
- Upload certificates to RB



File Name	Type	Size	Creation Time
[redacted]	script	57.6 KiB	Dec/16/2016 10:41:32
[redacted]	script	57.1 KiB	Oct/21/2016 15:18:21
[redacted]	backup	266.0 KiB	Oct/21/2016 15:17:42
[redacted]	backup	267.5 KiB	Dec/16/2016 10:40:56
[redacted]	.txt file	54.5 KiB	Jan/13/2017 13:26:23
[redacted]	.txt file	172.1 KiB	Jan/13/2017 11:12:53
[redacted]	.crt file	6.9 KiB	Aug/18/2015 16:06:17
[redacted]	.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 KiB	Dec/23/2016 09:21:22
pub	directory		Jan/02/1970 07:12:32
siteA-rb.crt	.crt file	6.9 KiB	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)



1

Only File: ca.crt

Passphrase: **********

2

Only File: siteA-rb.crt

Passphrase: **********

3

Only File: siteA-rb.key

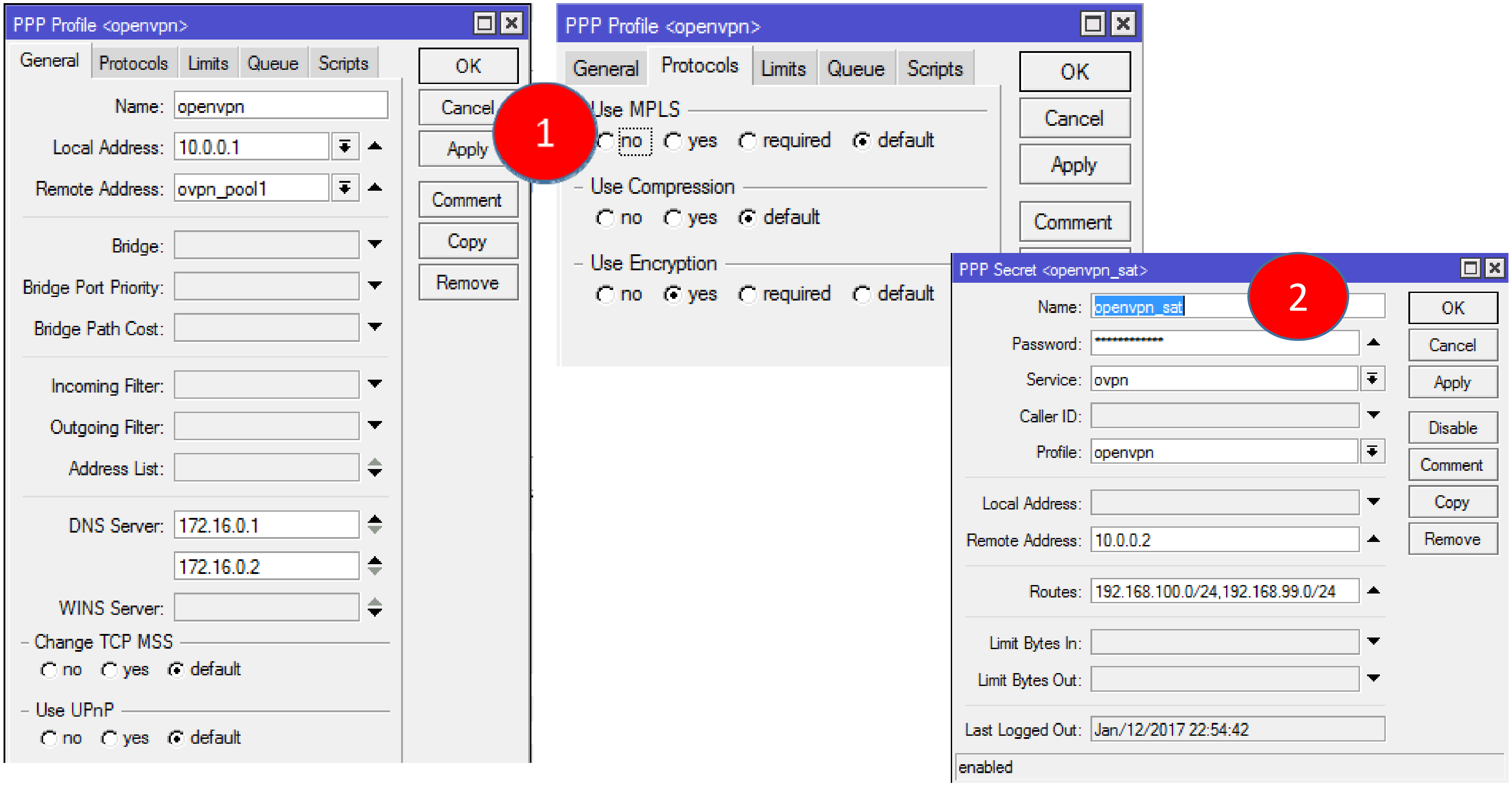
Passphrase: **********

4

	Name	Issuer	Common Name
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)



PPP Profile <openvpn>

Name: openvpn
Local Address: 10.0.0.1
Remote Address: ovpn_pool1
Bridge:
Bridge Port Priority:
Bridge Path Cost:
Incoming Filter:
Outgoing Filter:
Address List:
DNS Server: 172.16.0.1
172.16.0.2
WINS Server:

Change TCP MSS
○ no ○ yes ● default

Use UPnP
○ no ○ yes ● default

PPP Profile <openvpn>

Use MPLS
○ no ○ yes ○ required ● default

Use Compression
○ no ○ yes ● default

Use Encryption
○ no ● yes ○ required ○ default

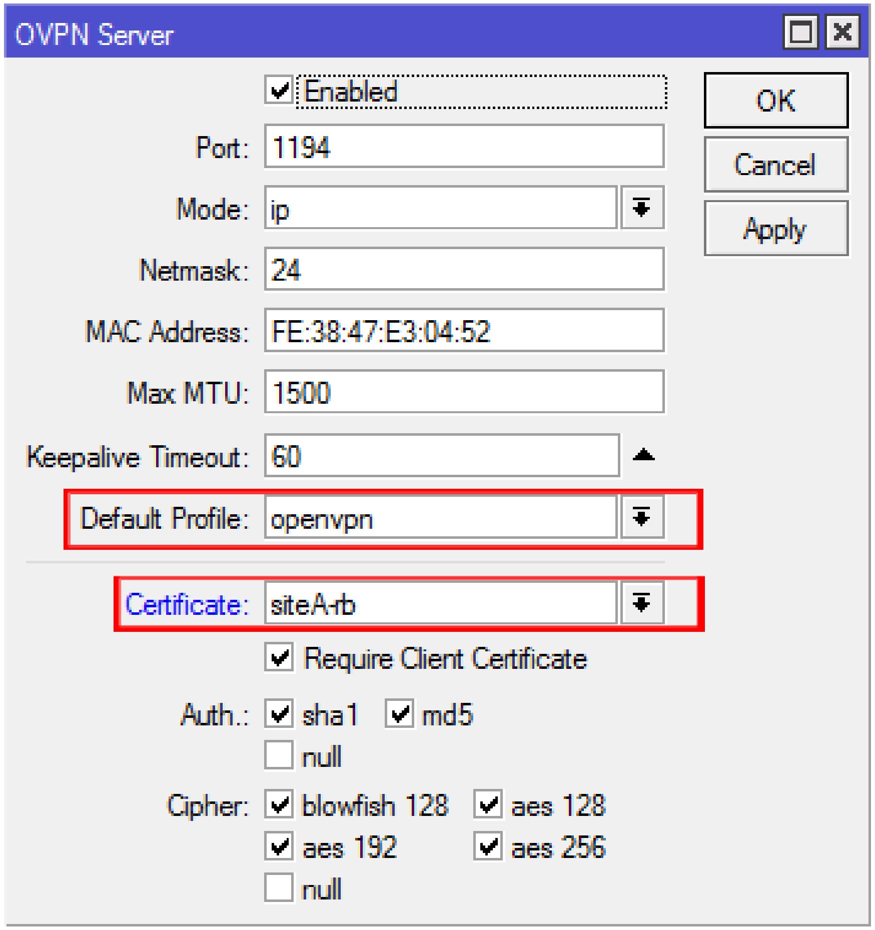
PPP Secret <openvpn_sat>

Name: openvpn_sat
Password: ************
Service: ovpn
Caller ID:
Profile: openvpn
Local Address:
Remote Address: 10.0.0.2
Routes: 192.168.100.0/24,192.168.99.0/24
Limit Bytes In:
Limit Bytes Out:
Last Logged Out: Jan/12/2017 22:54:42

enabled

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

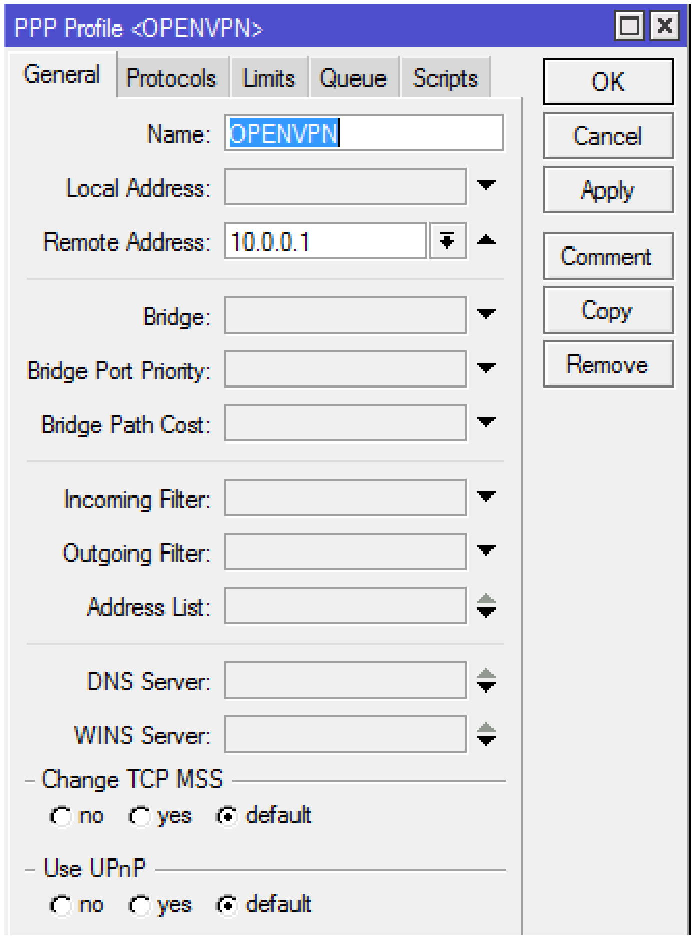
Auth.: ☑ sha1 ☑ md5 □ null

Cipher: ☑ blowfish 128 ☑ aes 128 ☑ aes 192 ☑ aes 256 □ null

- 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

Name: OPENVPN

Local Address:

Remote Address: 10.0.0.1

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Incoming Filter:

Outgoing Filter:

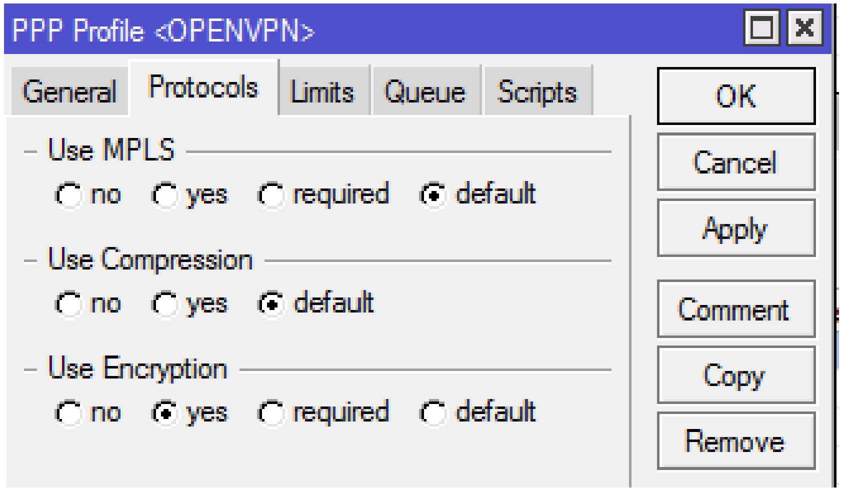
Address List:

DNS Server:

WINS Server:

Change TCP MSS: ○ no ○ yes ● default

Use UPnP: ○ no ○ yes ● default



PPP Profile <OPENVPN>

Protocols

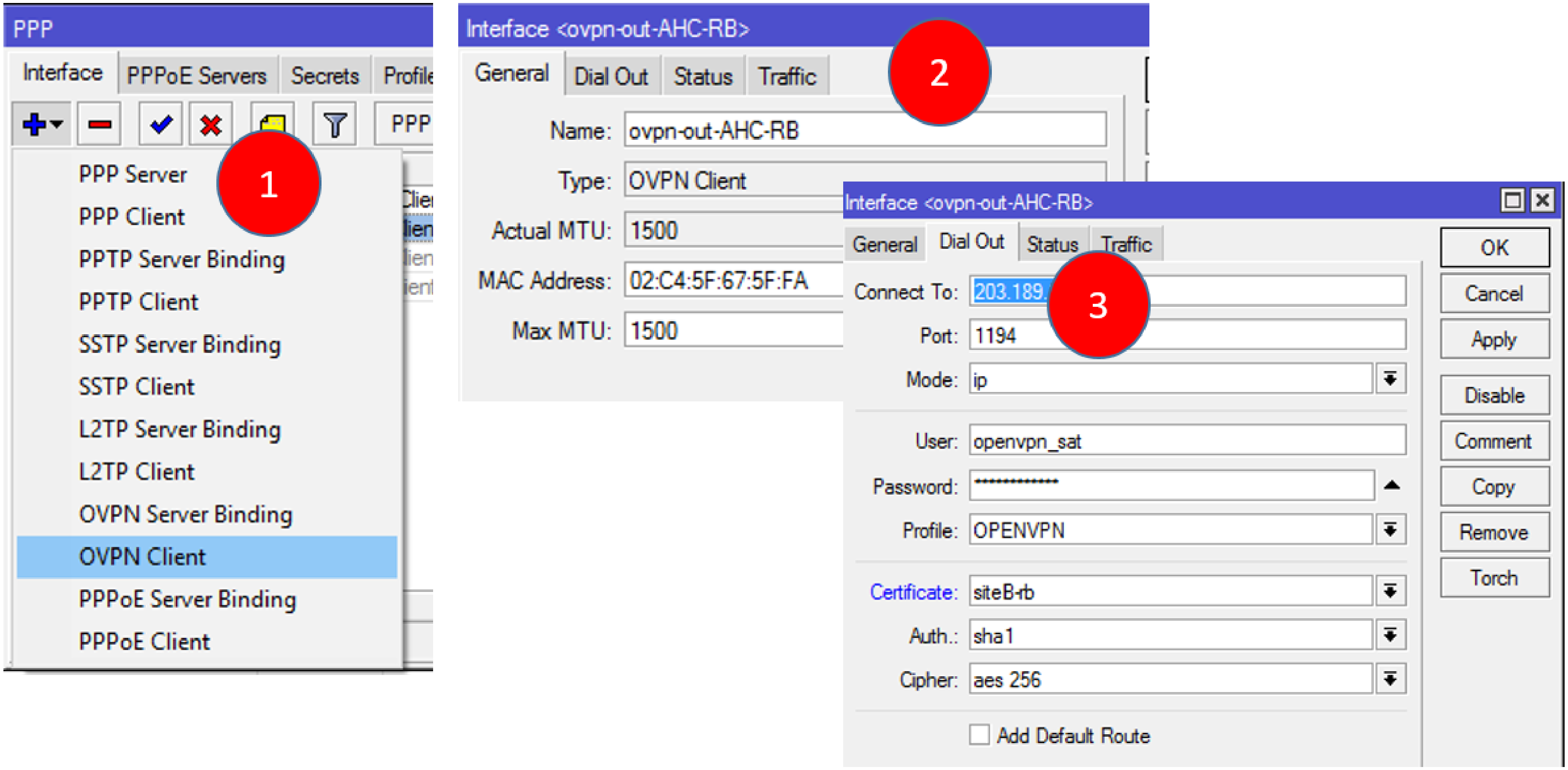
Use MPLS: ○ no ○ yes ○ required ● default

Use Compression: ○ no ○ yes ● default

Use Encryption: ○ no ● yes ○ required ○ default

Step 5: Configure OVPN client on RB at Site B

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



Interface <ovpn-out-AHC-RB>

Name: ovpn-out-AHC-RB

Type: OVPN Client

Actual MTU: 1500

MAC Address: 02:C4:5F:67:5F:FA

Max MTU: 1500

Interface <ovpn-out-AHC-RB>

Connect To: 203.189.

Port: 1194

Mode: ip

User: openvpn_sat

Password: *************

Profile: OPENVPN

Certificate: siteB-rb

Auth.: sha1

Cipher: aes 256

□ Add Default Route

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