

Implement Split Tunneling with Mikrotik



Hello World...

- Yosef Isa Pangestu
- Technical Consultant at PT. Wahana Ciptasinatria, Security & Network Division
- Graduated from STMIK Bani Saleh

Virtual Private Connection (VPN)

- Nowadays, it's used for WAN over Internet
- Commonly used by road warriors (Mobile User)
- Securing to access internal traffic through internet
- Mikrotik support Protocols VPN : PPTP, L2TP, SSTP, IPSec, OVPN, PPPoE, EoIP, GRE Tunnel, IP Tunnel

Mikrotik – SSTP VPN

- Provides PPP traffic through an SSL/TLS channel
- TCP 443
- Available for Linux, BSD, Windows
- Require Certificate to deploy
- Support authentication user by Local Database / LDAP/ Active Directory

Somedays..

- Company A has a HO and a few branches different sites
- Every sites need to be connected to HO for their internal application requirements
- Need to secure the internal application and data
- Internet at HO has more bandwidth and dedicated IP
- Allow only to access internal network from mobile users
- Budget extend will be going on unpredictable time
- The Routers is Mikrotik RouterOS

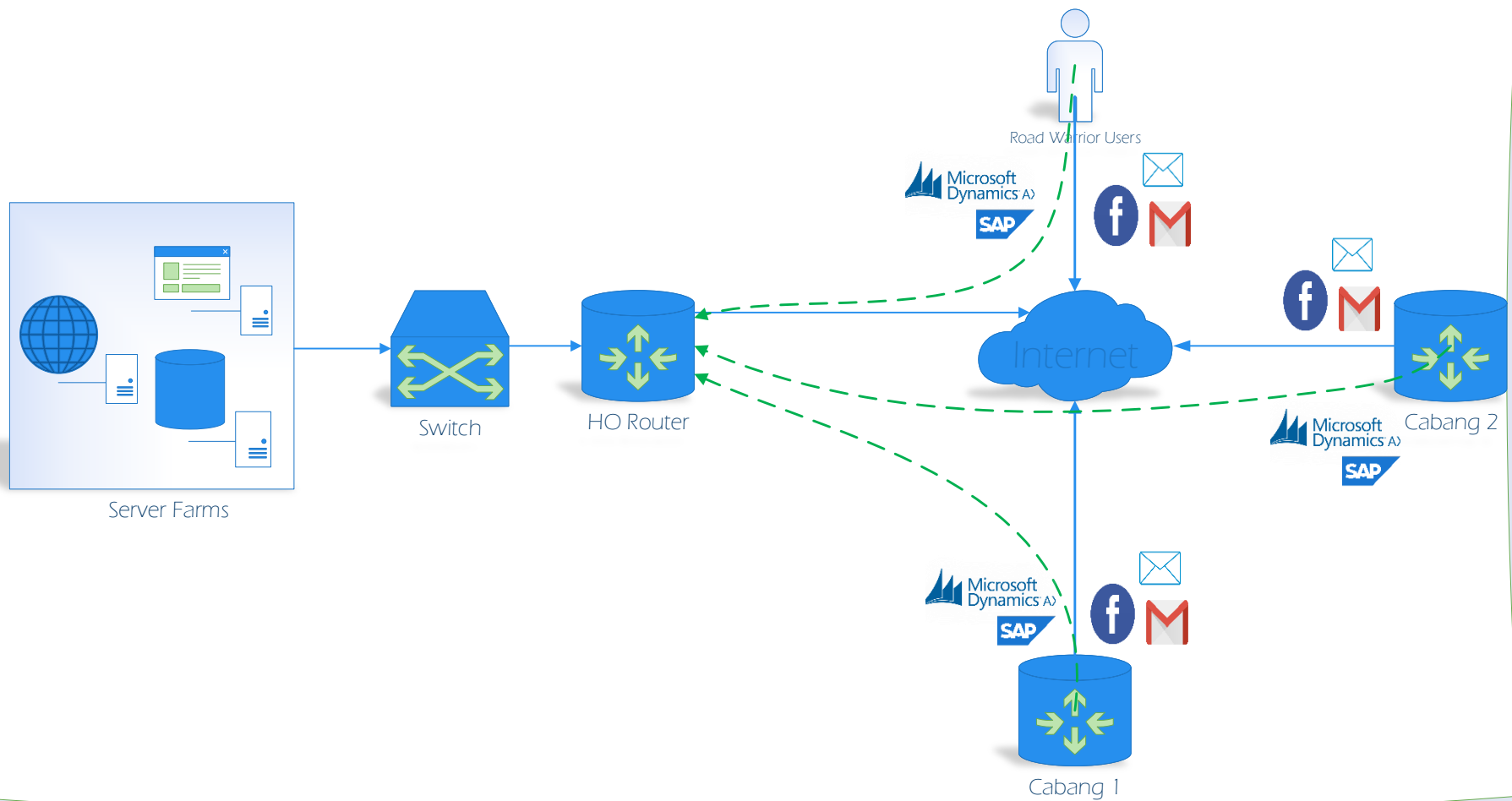


Split Tunnel

- Access internal network through the VPN, at the same time using the different network connections
- Lets you route some of your device or app traffic through the VPN while other device or apps maintain direct access to the internet

Scenario

Topology



We do at some points..

- Deployment on Mikrotik HO :
 - Certificates
 - DHCP IP Pool
 - PPP Profile
 - PPP Secret
 - Configure SSTP Server
- Configure Split Tunnel on Mikrotik Branch
- Configure Split Tunnel on Endpoint (Windows)



Mikrotik – Configure Mikrotik HO

Certificate <CA>

General Key Usage Status

Name: CA

Issuer:

Country: ID

State: DKI Jakarta

Locality: na

Organization: na

Unit: na

Common Name: vpnsrv.mycorps.local

Subject Alt. Name: IP : ::

Key Size: 2048

Days Valid: 365

OK
Cancel
Apply
Copy
Remove
Sign
Sign via SCEP
Import
Card Reinstall
Card Verify
Set CA Passphrase
Export
Revoke

private key | crl | authority | expired | smart card k | trusted

New Certificate

General Key Usage Status

Key Usage:

- ☐ digital signature
- ☐ key encipherment
- ☐ key agreement
- ☒ crl sign
- ☐ decipher only
- ☐ server gated crypto
- ☐ timestamp
- ☐ ipsec tunnel
- ☐ email protect
- ☐ tls client
- ☐ content commitment
- ☐ data encipherment
- ☒ key cert. sign
- ☐ encipher only
- ☐ dvcs
- ☐ ocsp sign
- ☐ ipsec user
- ☐ ipsec end system
- ☐ code sign
- ☐ tls server

OK
Cancel
Apply
Copy
Remove
Sign
Sign via SCEP
Import
Card Reinstall
Card Verify
Set CA Passphrase
Export
Revoke

private key | crl | authority | expired | smart card k | trusted

Create Certificate Root CA Self Signed

Certificate <Server>

General Key Usage Status

Name:

Issuer:

Country:

State:

Locality:

Organization:

Unit:

Common Name:

Subject Alt. Name: : ::

Key Size:

Days Valid:

☒ Trusted

OK
Cancel
Apply
Copy
Remove
Sign
Sign via SCEP
Import
Card Reinstall
Card Verify
Set CA Passphrase
Export
Revoke

private key crl authority issued expired smart card key trusted

Sign

Certificate: ▼

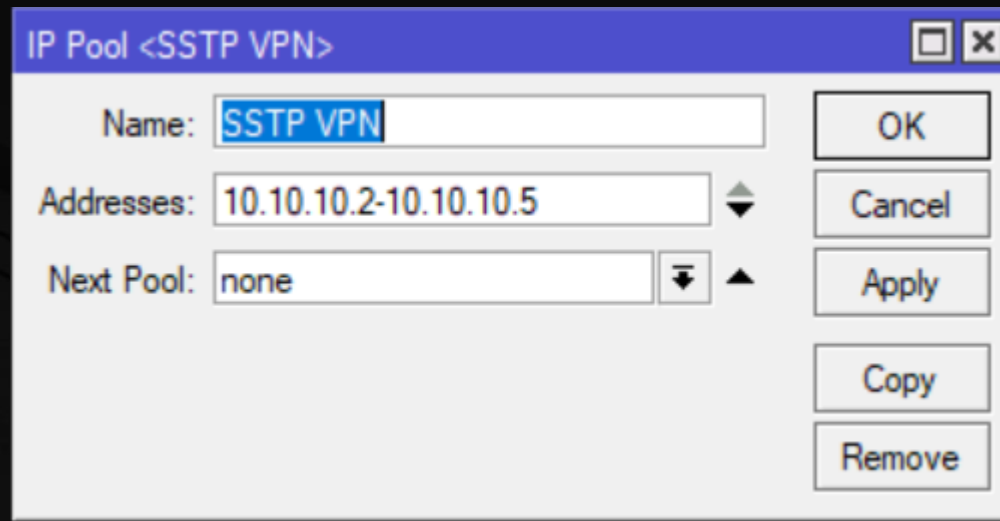
CA: ▼ ▲

CA CRL Host:

Progress:

Start
Stop
Close

Create Certificate Server Self Signed



The image shows a Windows-style dialog box titled "IP Pool <SSTP VPN>". It contains three input fields: "Name" with the value "SSTP VPN", "Addresses" with the value "10.10.10.2-10.10.10.5", and "Next Pool" with the value "none". To the right of these fields are five buttons: "OK", "Cancel", "Apply", "Copy", and "Remove". The "Next Pool" field has a dropdown arrow on its right side.

IP Pool <SSTP VPN>

Name: SSTP VPN

Addresses: 10.10.10.2-10.10.10.5

Next Pool: none

OK

Cancel

Apply

Copy

Remove

Create IP DHCP Pool for SSTP Clients

New PPP Profile

General Protocols Limits Queue Scripts

Name: split-vpn

Local Address: 10.10.10.1

Remote Address: SSTP VPN

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Bridge Horizon:

Incoming Filter:

Outgoing Filter:

Address List:

Interface List:

DNS Server:

WINS Server:

- Change TCP MSS

☐ no ☐ yes ☒ default

- Use UPnP

☐ no ☐ yes ☒ default

OK Cancel Apply Comment Copy Remove

New PPP Profile

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

Create PPP Profile for SSTP Clients

PPP Secret <isa>

Name: isa

Password:

Service: sstp

Caller ID:

Profile: split-vpn

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out: Feb/17/2018 13:24:28

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Create Username for Mobile Users and Mikrotik Branch

SSTP Server

☒ Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU: ▼

Keepalive Timeout: 60 ▲

Default Profile: split-vpn ▼

Authentication: ☒ mschap2 ☐ mschap1
☐ chap ☐ pap

Certificate: Server ▼

TLS Version: only-1.2 ▼

☐ Verify Client Certificate

☒ Force AES

☒ PFS

OK

Cancel

Apply

Enable SSTP Server Interface on Mikrotik HO



Mikrotik – Configure Mikrotik Branch as Split Tunneling VPN

Certificate <cert_export_CA.crt_0>

General Key Usage Status

Name: cert_export_CA.crt_0

Issuer: C=ID,ST=DKI Jakarta,L=na,O=na,OU=na,CN=vpnsvr.mycorps.local

Country: ID

State: DKI Jakarta

Locality: na

Organization: na

Unit: na

Common Name: vpnsvr.mycorps.local

Subject Alt. Name: unknown : ::

Key Size: 2048

Days Valid: 365

☒ Trusted

private key crt authority expired smart card key trusted

OK
Cancel
Apply
Copy
Remove
Sign
Sign via SCEP
Import
Card Reinstall
Card Verify
Set CA Passphrase
Export
Revoke

Import Certificate Root CA + Private Key Mikrotik HO

Interface <split-tunnel-toHO>

General Dial Out Status Traffic

Connect To:

Port:

Proxy:

Proxy Port:

Certificate:

TLS Version:

☐ Verify Server Certificate

☒ Verify Server Address From Certificate

☐ PFS

User:

Password:

Profile:

Keepalive Timeout:

☐ Dial On Demand

☐ Add Default Route

Default Route Distance:

Allow: ☒ mschap2 ☐ mschap1

☐ chap ☐ pap

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Torch

enabled running slave Status: connected

Create new SSTP Client interface

/ip firewall mangle

add action=mark-routing chain=prerouting dst-address=192.168.100.0/24
new-routing-mark=split-to-ho passthrough=no protocol=icmp

add action=mark-routing chain=prerouting dst-address=192.168.100.0/24
dst-port=443 new-routing-mark=split-to-ho passthrough=no protocol=tcp

/ip route

add distance=1 dst-address=192.168.1.0/24 gateway=split-tunnel-toHO
routing-mark=split-to-ho

Result – Split the connection

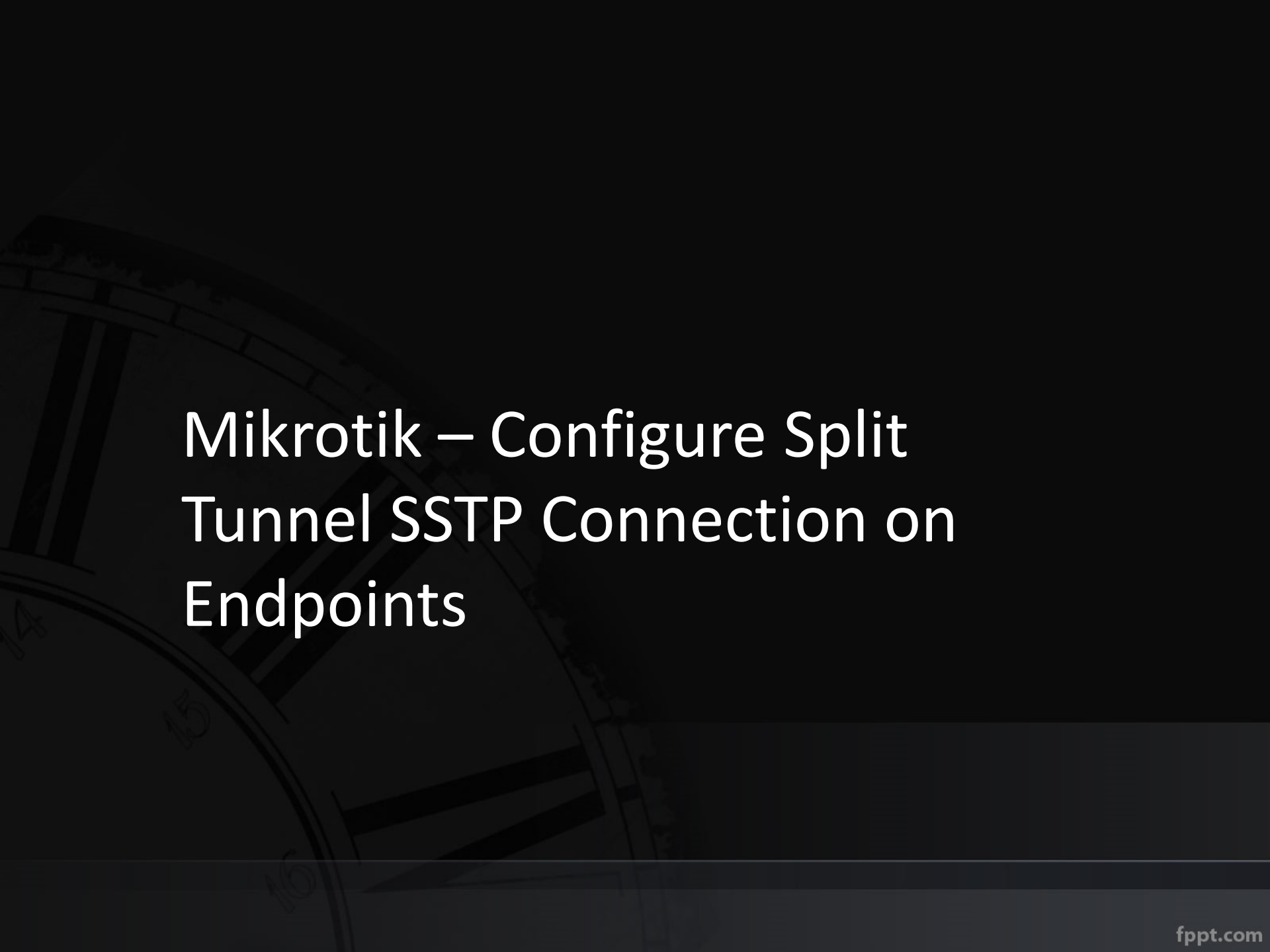
```
[admin@MikroTik] > tool traceroute 8.8.8.8
```

#	ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST	STD-DEV	STATUS
1	192.168.100.1	0%	4	1.7ms	1.6	1.4	1.8	0.1	
2	10.89.0.1	0%	4	4.4ms	4.3	4	4.6	0.2	
3		100%	4	timeout					
4		100%	3	timeout					
5	203.176.181.229	0%	3	6.4ms	6.1	5.9	6.4	0.2	
6	103.66.199.54	0%	3	24.1ms	24.5	24.1	24.7	0.3	
7	72.14.215.17	0%	3	24.2ms	24.1	23.8	24.2	0.2	
8	108.170.254.225	0%	3	18.5ms	18.6	18.3	19.1	0.3	
9	64.233.175.69	0%	3	20.3ms	20.1	20	20.3	0.1	
10	8.8.8.8	0%	3	24.6ms	24.4	24.1	24.6	0.2	

```
[admin@MikroTik] >  
[admin@MikroTik] >  
[admin@MikroTik] > tool traceroute 192.168.100.1
```

#	ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST	STD-DEV	STATUS
1	192.168.100.1	0%	4	2.2ms	2	1.3	2.5	0.4	

```
[admin@MikroTik] > █
```

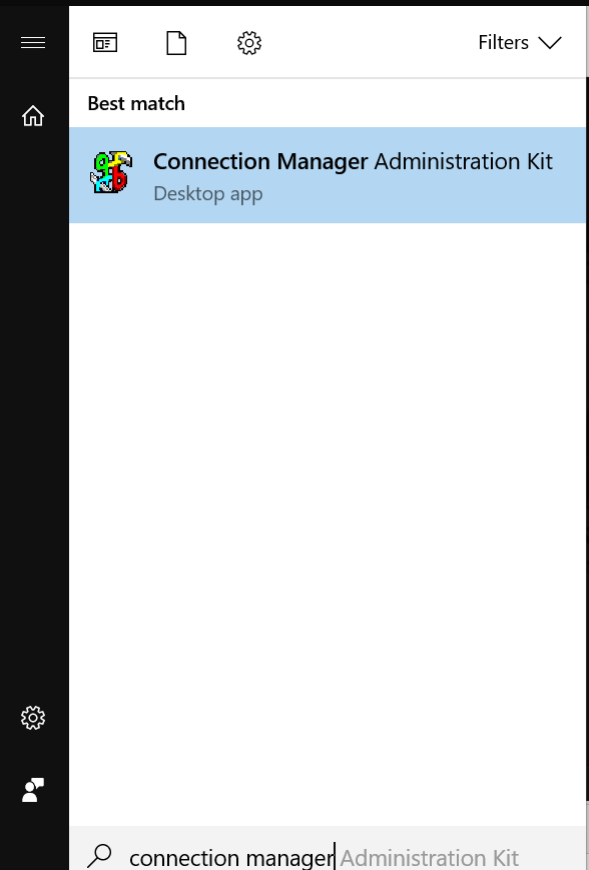
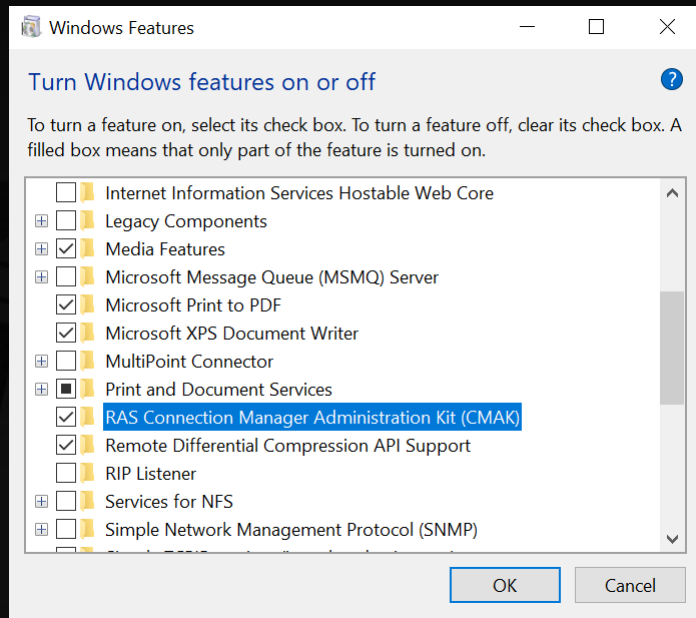


Mikrotik – Configure Split Tunnel SSTP Connection on Endpoints

How do we split route on endpoints?

On >100 endpoints?





Create Executable Files VPN Profile with CMAK

Connection Manager Administration Kit Wizard

Add a Custom Phone Book

A phone book is a collection of access numbers that users can dial to connect to a remote dial-up network. A phone book file can be automatically updated each time the user connects with this profile.

To include a phone book, specify the name of the .pbk file. Confirm that there is a corresponding .pbr file in the same folder. You can use Phone Book Administrator (PBA) in Connection Point Services to create and manage phone book files.

Phone book file:

☐ Automatically download phone book updates

Type the text you want to appear next to the More access numbers box in the Phone Book dialog box.

More access numbers text:

Example: There is a surcharge to dial these numbers.

< Back

Next >

Cancel

Connection Manager Administration Kit Wizard

Configure Dial-up Networking Entries

A dial-up networking entry contains additional configuration information for one or more phone numbers in the phone book, including IP settings to use and scripts to run.

Specify the dial-up networking entry that you want to customize. You must type each entry name exactly as it appears in the phone book for this Connection Manager profile.

Dial-up networking entries:

VPN SSTP My Corps <Default>

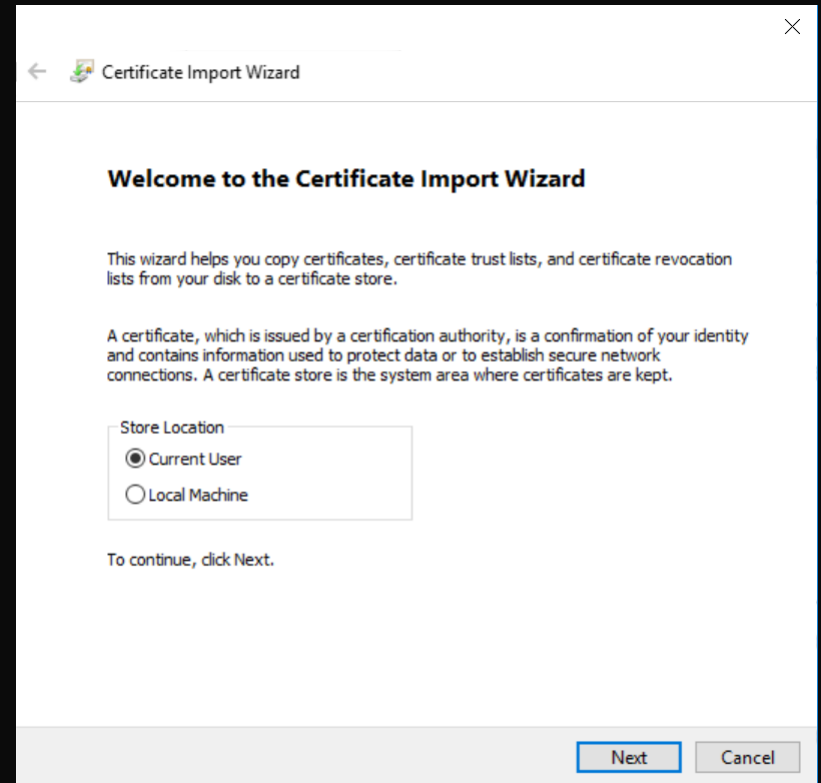
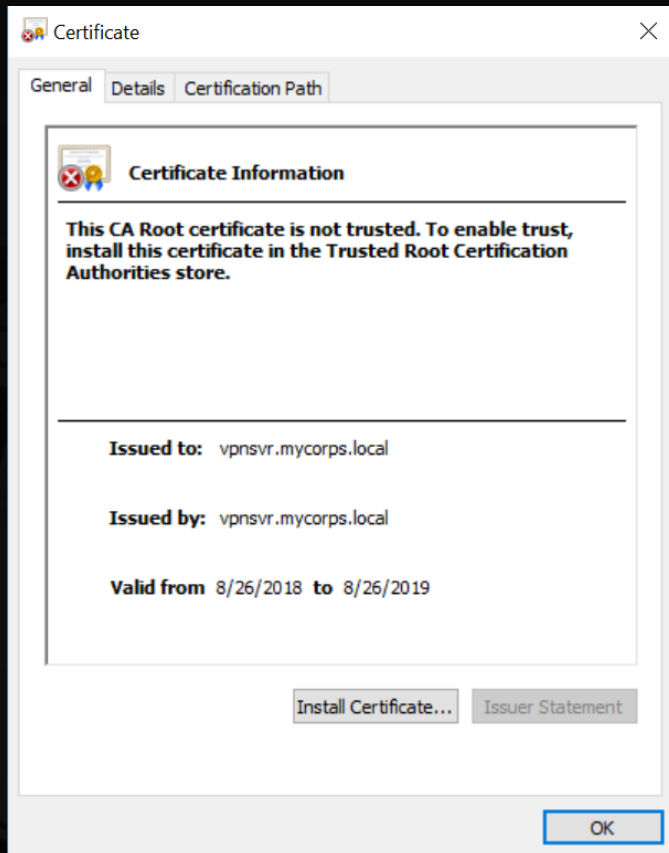
< Back

Next >

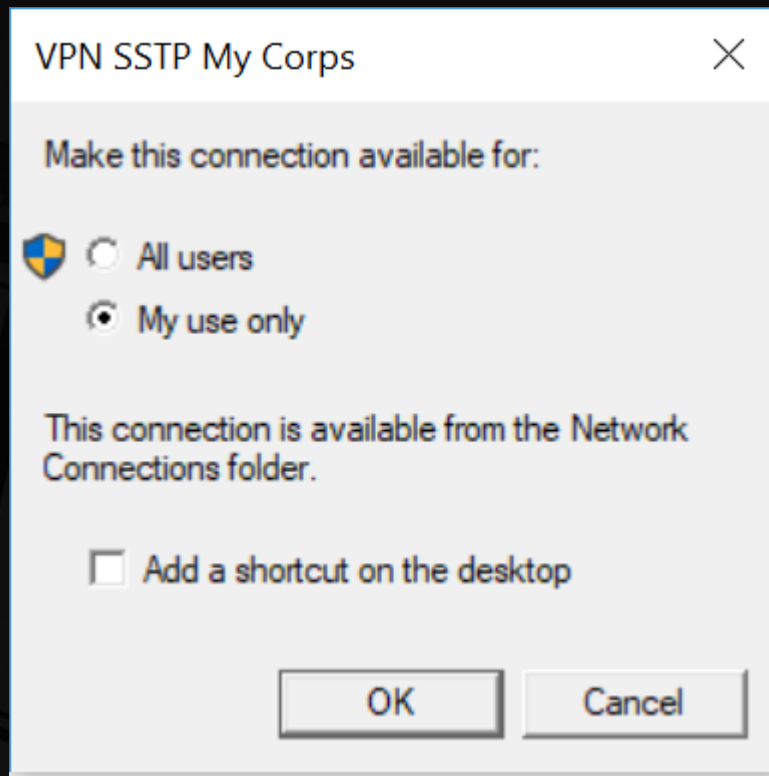
Cancel

Create Route Table Profile for SSTP Client Interface

- Create a new txt file
- Define the routes will be through the VPN
- i.e -> `ADD 192.168.100.0 MASK 255.255.255.0 default METRIC default IF default`
- Save the file with .txt name
- Then, choose the file on CMAK

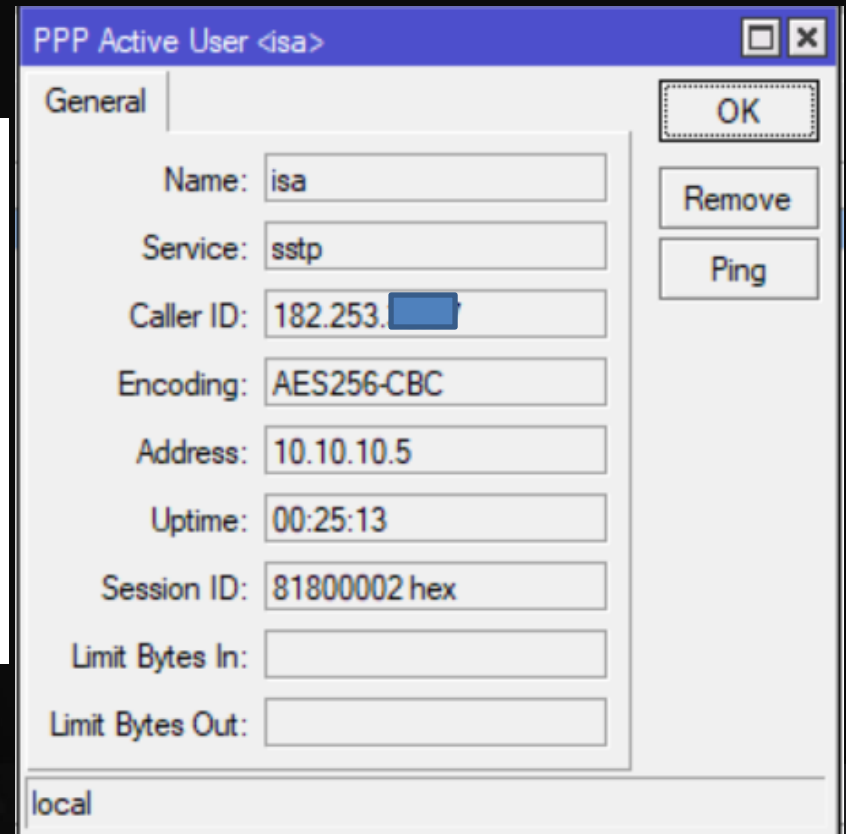
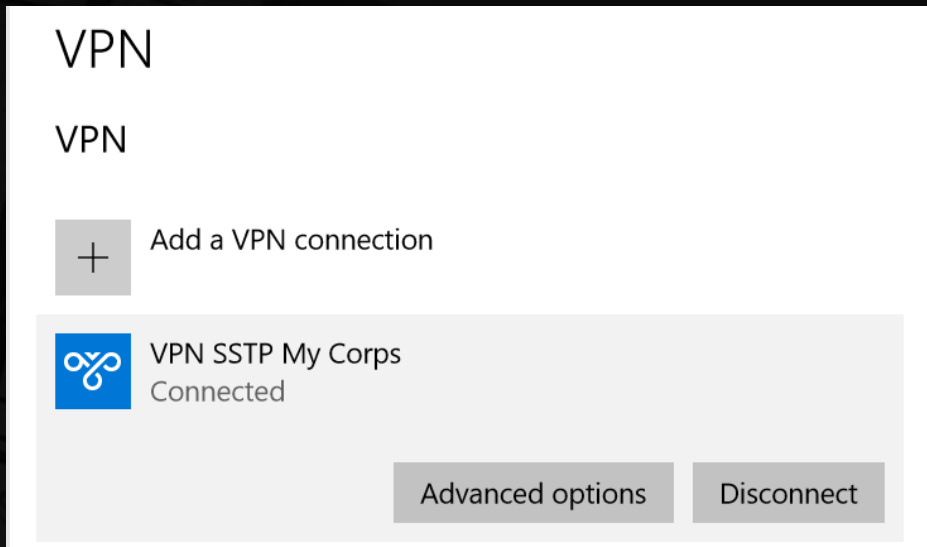


Import Certificate Root CA Mikrotik HO



Install the executable file VPN SSTP Profile

Result – Without Split Tunnel



IPv4 Route Table

=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	10.10.4.1	10.10.4.15	4260
0.0.0.0	0.0.0.0	0.0.0.0	On-link	10.10.10.4	36
10.10.4.0	255.255.255.0	255.255.255.0	On-link	10.10.4.15	4516
10.10.4.15	255.255.255.255	255.255.255.255	On-link	10.10.4.15	4516
10.10.4.255	255.255.255.255	255.255.255.255	On-link	10.10.4.15	4516
10.10.10.4	255.255.255.255	255.255.255.255	On-link	10.10.10.4	291
10.103.6.2	255.255.255.255	255.255.255.255	10.10.4.1	10.10.4.15	4261
127.0.0.0	255.0.0.0	255.0.0.0	On-link	127.0.0.1	4556
127.0.0.1	255.255.255.255	255.255.255.255	On-link	127.0.0.1	4556
127.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	4556
192.168.56.0	255.255.255.0	255.255.255.0	On-link	192.168.56.1	4506
192.168.56.1	255.255.255.255	255.255.255.255	On-link	192.168.56.1	4506
192.168.56.255	255.255.255.255	255.255.255.255	On-link	192.168.56.1	4506
192.168.137.0	255.255.255.0	255.255.255.0	On-link	192.168.137.1	4536
192.168.137.1	255.255.255.255	255.255.255.255	On-link	192.168.137.1	4536
192.168.137.255	255.255.255.255	255.255.255.255	On-link	192.168.137.1	4536
192.168.220.0	255.255.255.0	255.255.255.0	On-link	192.168.220.1	4516
192.168.220.1	255.255.255.255	255.255.255.255	On-link	192.168.220.1	4516
192.168.220.255	255.255.255.255	255.255.255.255	On-link	192.168.220.1	4516
192.168.225.0	255.255.255.0	255.255.255.0	On-link	192.168.225.1	4516
192.168.225.1	255.255.255.255	255.255.255.255	On-link	192.168.225.1	4516
192.168.225.255	255.255.255.255	255.255.255.255	On-link	192.168.225.1	4516
224.0.0.0	240.0.0.0	240.0.0.0	On-link	127.0.0.1	4556
224.0.0.0	240.0.0.0	240.0.0.0	On-link	192.168.56.1	4506
224.0.0.0	240.0.0.0	240.0.0.0	On-link	192.168.220.1	4516

```
C:\Users\ISA>tracert -d 8.8.8.8
```

```
Tracing route to 8.8.8.8 over a maximum of 30 hops
```

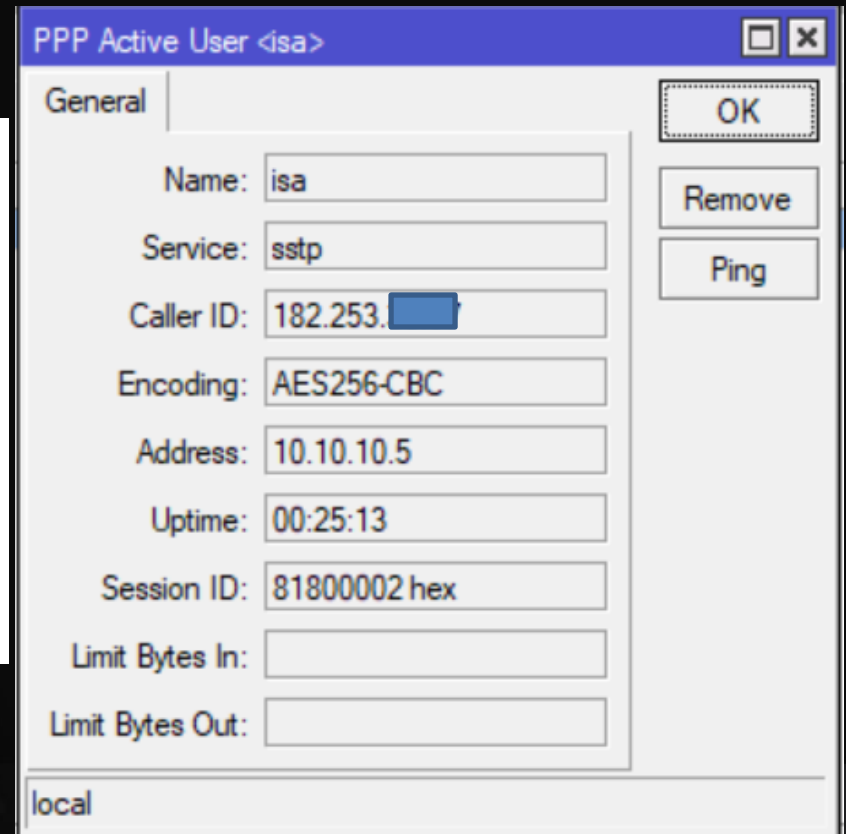
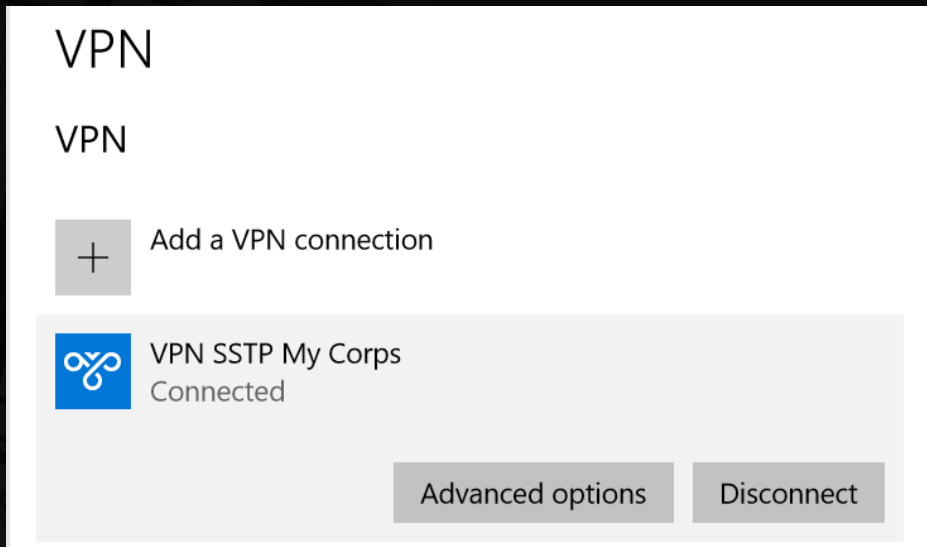
1	65 ms	129 ms	91 ms	10.10.10.1
2	53 ms	57 ms	117 ms	117.103.66.1
3	100 ms	77 ms	97 ms	203.79.29.33
4	85 ms	55 ms	99 ms	103.28.94.145
5	70 ms	70 ms	84 ms	103.28.94.2
6	81 ms	75 ms	77 ms	108.170.240.225
7	68 ms	125 ms	71 ms	108.170.233.71
8	101 ms	101 ms	75 ms	8.8.8.8

```
Trace complete.
```

```
C:\Users\ISA>
```

Routes without split the connection

Result – With Split Tunnel



IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	10.10.4.1	10.10.4.15	35
10.0.0.0	255.0.0.0		10.10.10.1	10.10.10.5	36
10.10.4.0	255.255.255.0		On-link	10.10.4.15	291
10.10.4.15	255.255.255.255		On-link	10.10.4.15	291
10.10.4.255	255.255.255.255		On-link	10.10.4.15	291
10.10.10.5	255.255.255.255		On-link	10.10.10.5	291
10.103.0.2	255.255.255.255		10.10.4.1	10.10.4.15	36
127.0.0.0	255.0.0.0		On-link	127.0.0.1	331
127.0.0.1	255.255.255.255		On-link	127.0.0.1	331
127.255.255.255	255.255.255.255		On-link	127.0.0.1	331
192.168.56.0	255.255.255.0		On-link	192.168.56.1	281
192.168.56.1	255.255.255.255		On-link	192.168.56.1	281
192.168.56.255	255.255.255.255		On-link	192.168.56.1	281
192.168.100.0	255.255.255.0		10.10.10.1	10.10.10.5	53
192.168.137.0	255.255.255.0		On-link	192.168.137.1	311
192.168.137.1	255.255.255.255		On-link	192.168.137.1	311
192.168.137.255	255.255.255.255		On-link	192.168.137.1	311
192.168.220.0	255.255.255.0		On-link	192.168.220.1	291
192.168.220.1	255.255.255.255		On-link	192.168.220.1	291
192.168.220.255	255.255.255.255		On-link	192.168.220.1	291
192.168.225.0	255.255.255.0		On-link	192.168.225.1	291
192.168.225.1	255.255.255.255		On-link	192.168.225.1	291
192.168.225.255	255.255.255.255		On-link	192.168.225.1	291

```
C:\Users\ISA>tracert -d 192.168.100.1
```

```
Tracing route to 192.168.100.1 over a maximum of 30 hops
```

```
  1      4 ms      4 ms      4 ms  192.168.100.1
```

```
Trace complete.
```

```
C:\Users\ISA>tracert -d 8.8.8.8
```

```
Tracing route to 8.8.8.8 over a maximum of 30 hops
```

```
  1      1 ms      1 ms      1 ms  10.10.4.1
  2      4 ms      3 ms      3 ms  182.253.32.1
  3      4 ms      3 ms      3 ms  182.253.187.145
  4      4 ms      5 ms      4 ms  112.78.171.85
  5     18 ms     17 ms     17 ms  182.253.255.114
  6     15 ms     15 ms     15 ms  72.14.210.144
  7     17 ms     17 ms     16 ms  108.170.254.225
  8     15 ms     15 ms     16 ms  64.233.175.89
  9     15 ms     15 ms     15 ms  8.8.8.8
```

```
Trace complete.
```

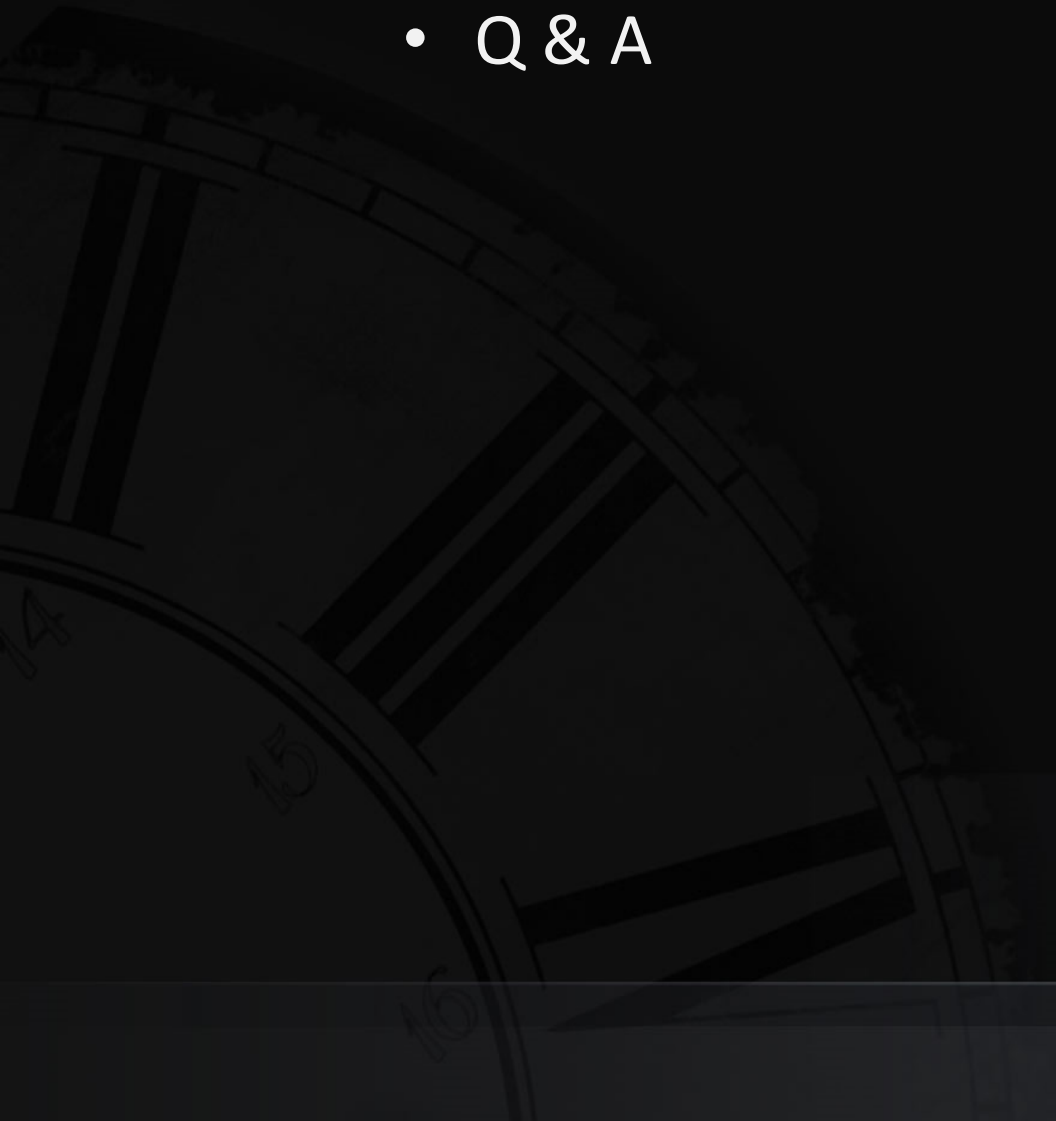
Routes with split the connection

Conclusion & Notes

- Minimize bandwidth utilization on HO Network from Road Warrior
- Split only traffic internal through VPN Connection
- Certificate can be using trusted CA to get effortless deployment
- Road warrior only split by IP Address, however Site-to-Site will able to be splited by ports and IP
- Able to massive deployment on endpoints with software deployment tools
- Secure to access internal network through Internet
- Port 443 is common with HTTPS so the firewall is not big deal to block or prevent

Thank you...

- Q & A



Reference

- https://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol
- http://www.mikrotik.co.id/artikel_lihat.php?id=206
- http://www.mikrotik.co.id/artikel_lihat.php?id=137
- <https://www.marthur.com/networking/mikrotik-setup-a-client-to-site-sstp-vpn-part-1/776/>
- <https://wiki.mikrotik.com/wiki/Manual:Interface/SSTP>
- <https://www.free-power-point-templates.com/>



<https://id.linkedin.com/in/isa-pangestu-5a52a097>



<https://www.instagram.com/voisapangestu/>



Isa.pangestu@outlook.com