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

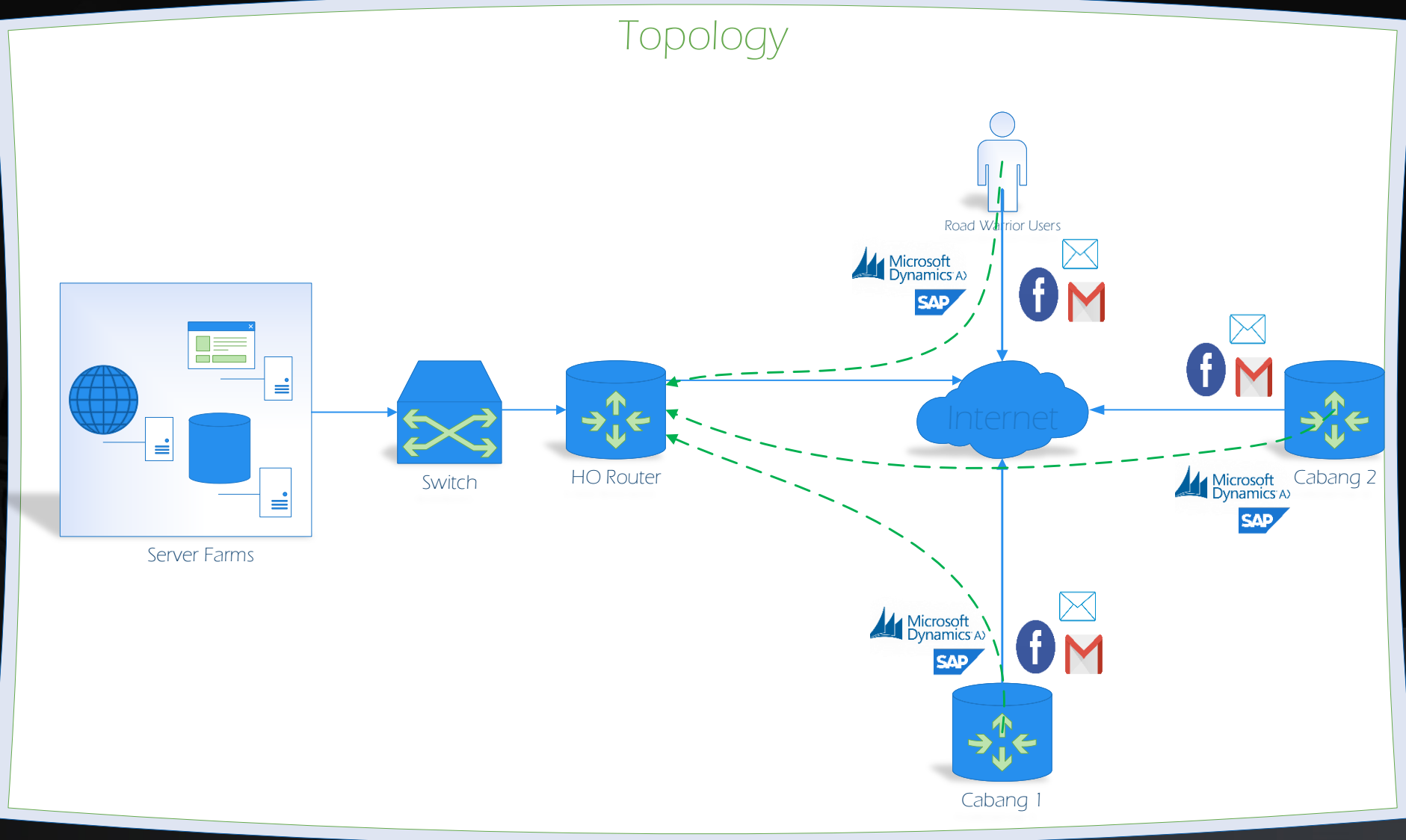
Somedays..

- 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 unpredictive 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

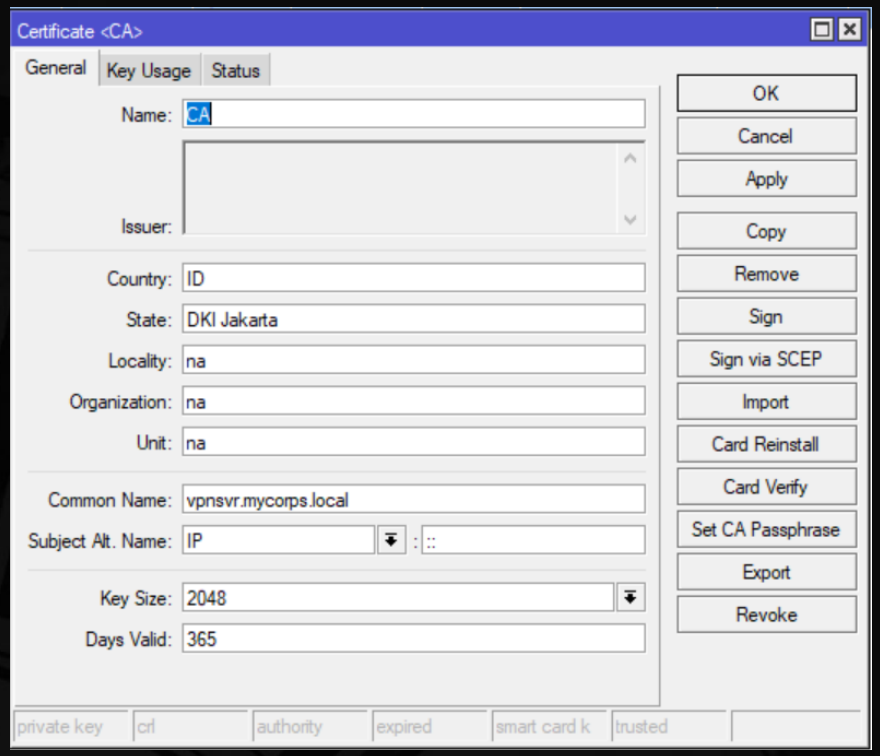
Scenario

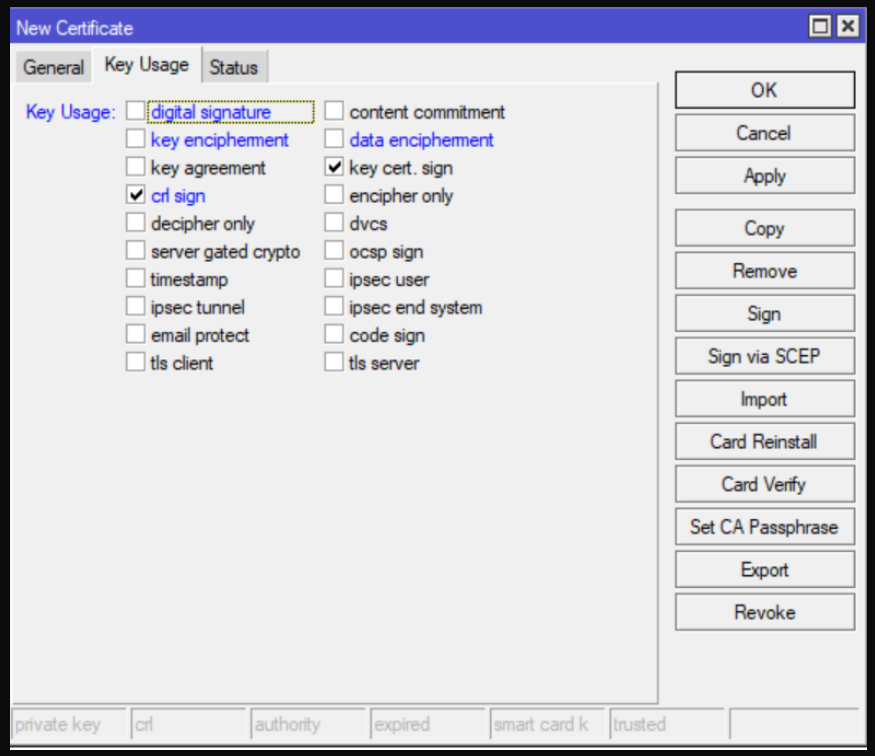


We do at some points..

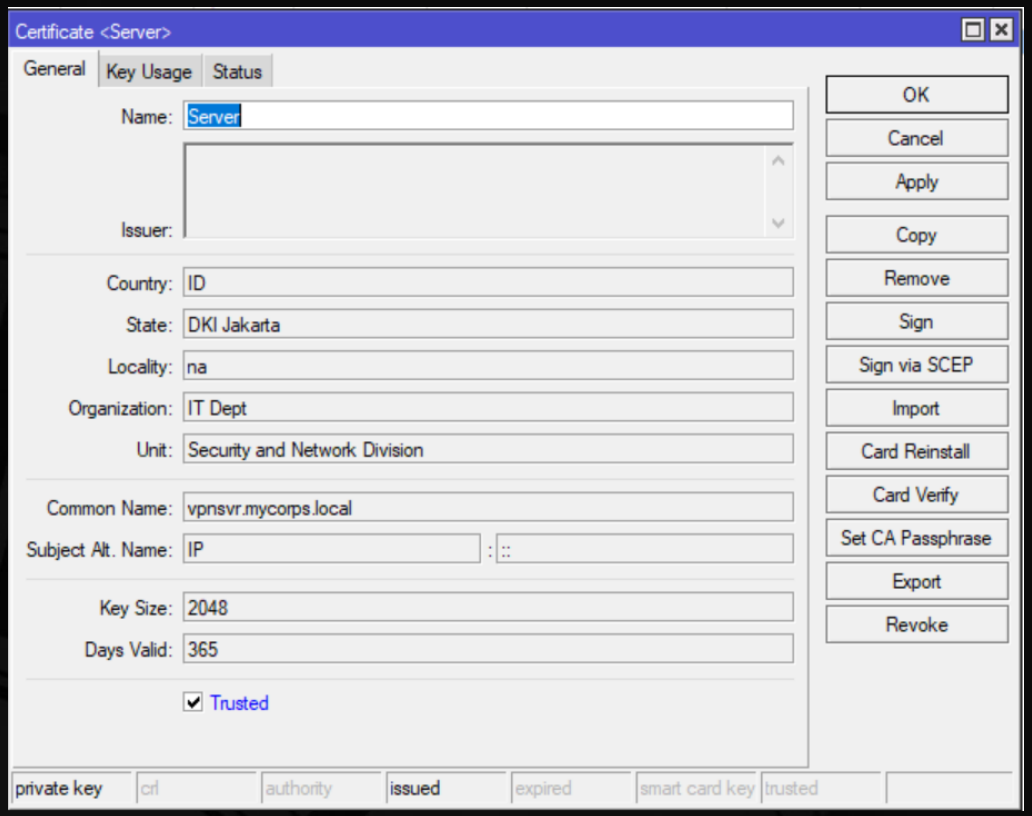
- Deployment on Mikrotik HO :
    - Certificates
    - DHCP IP Pool
    - PPP Profile
    - PPP Secret
    - Configure SSTP Server
- Configure Split Tunnel on Mikrotik Branch
- Configure Split Tunnel on Endpoint (Windows)

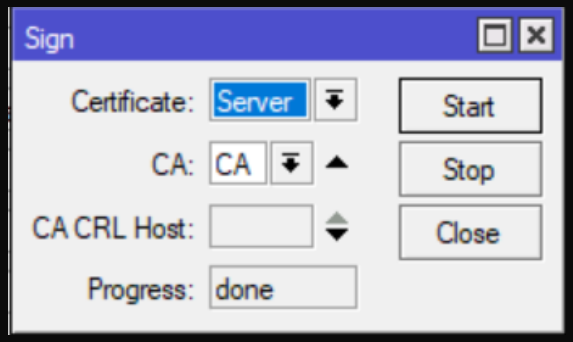
Mikrotik – Configure Mikrotik HO



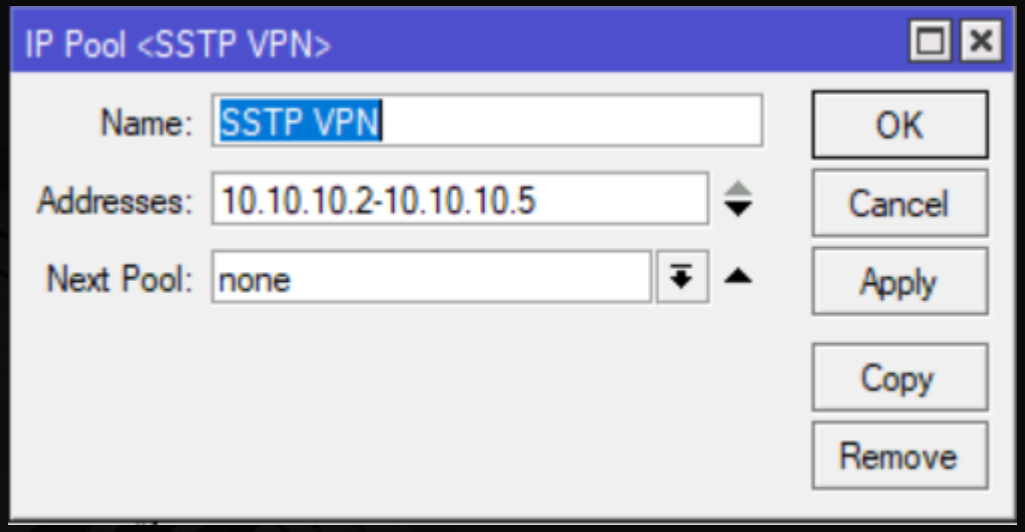


Create Certificate Root CA Self Signed

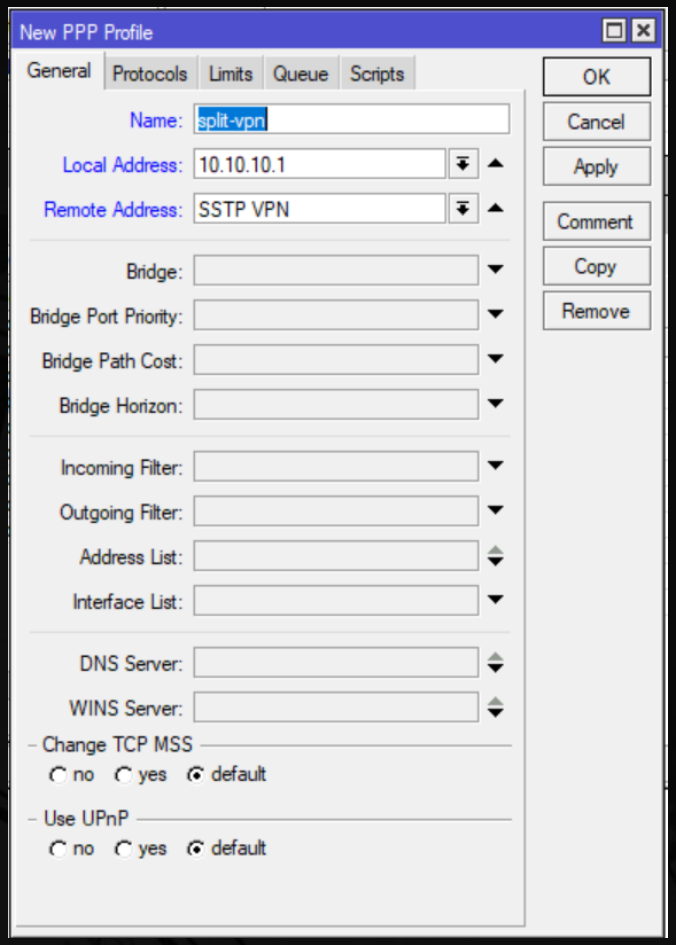


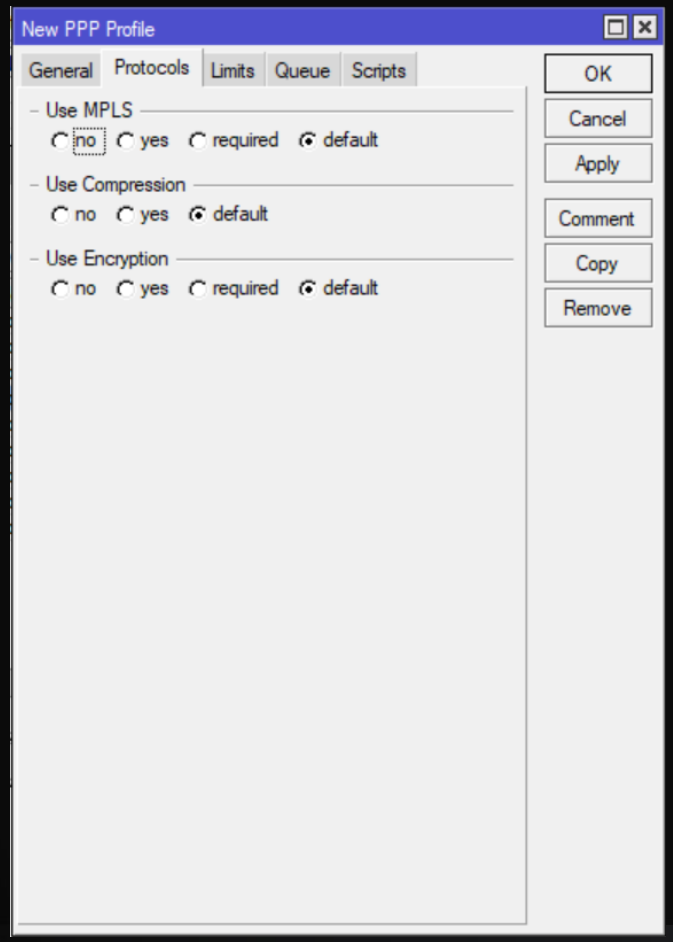


Create Certificate Server Self Signed

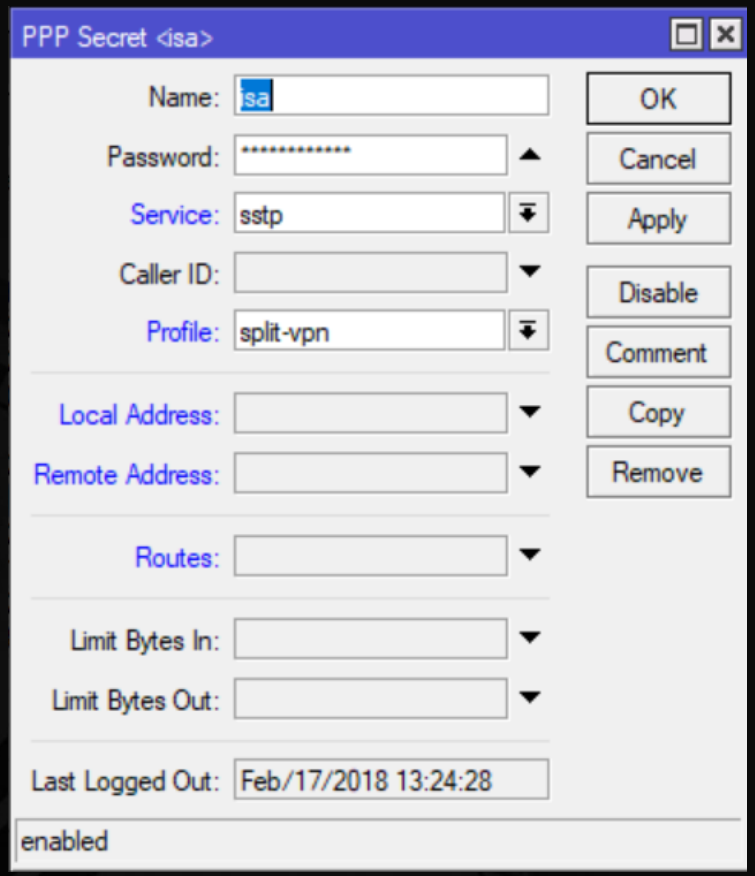


Create IP DHCP Pool for SSTP Clients

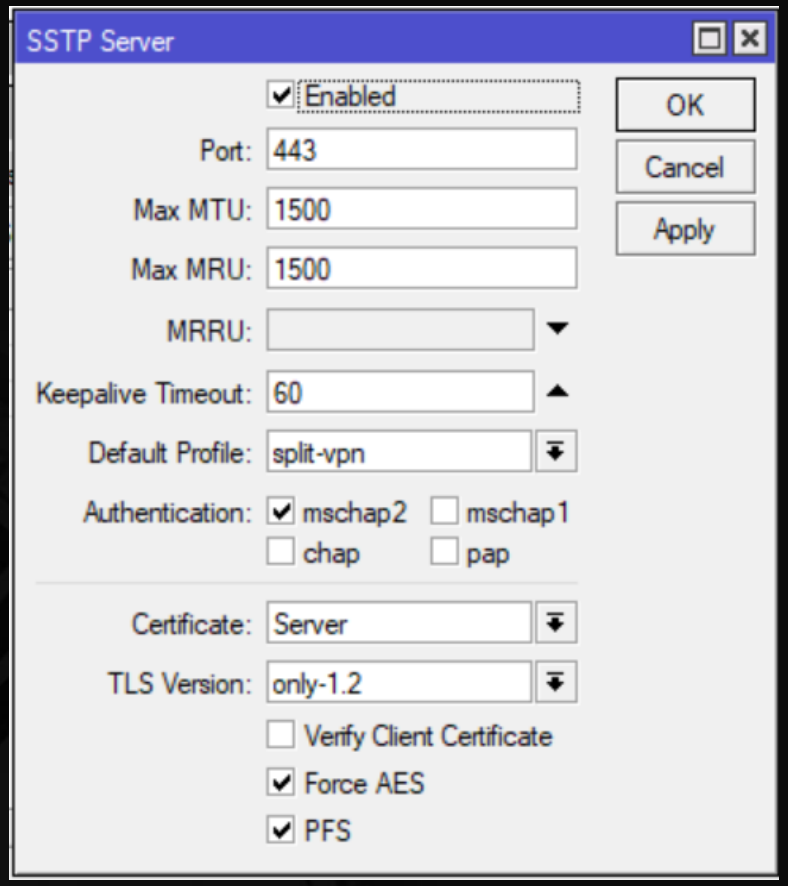




Create PPP Profile for SSTP Clients

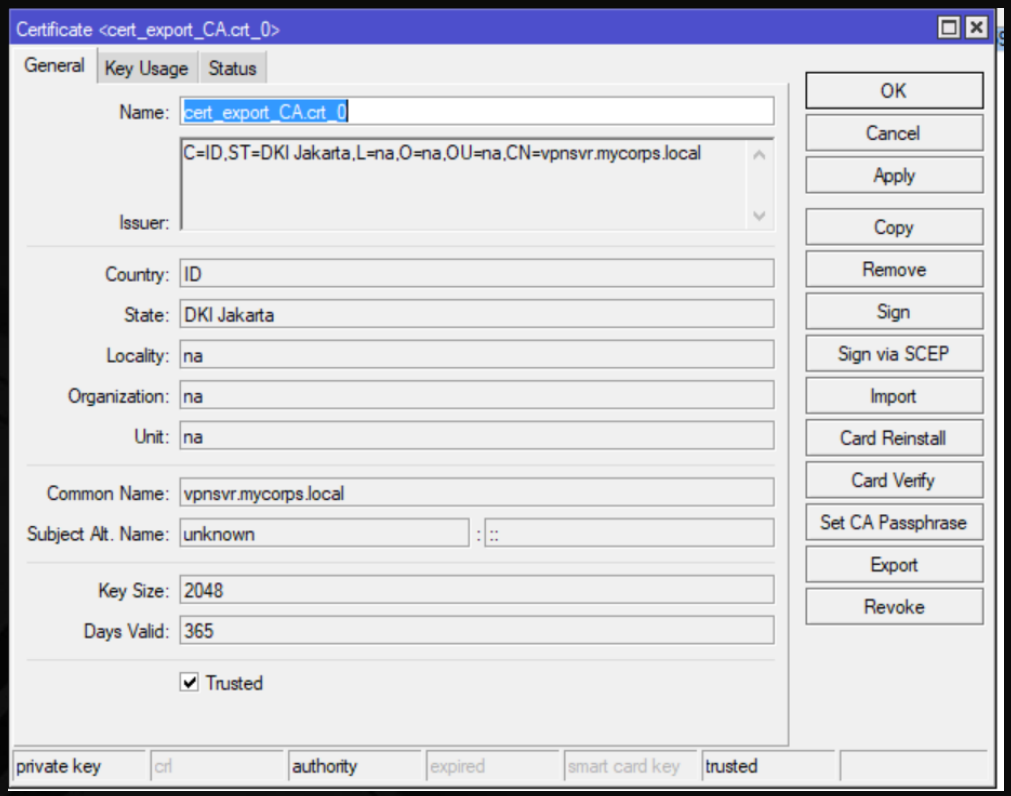


Create Username for Mobile Users and Mikrotik Branch

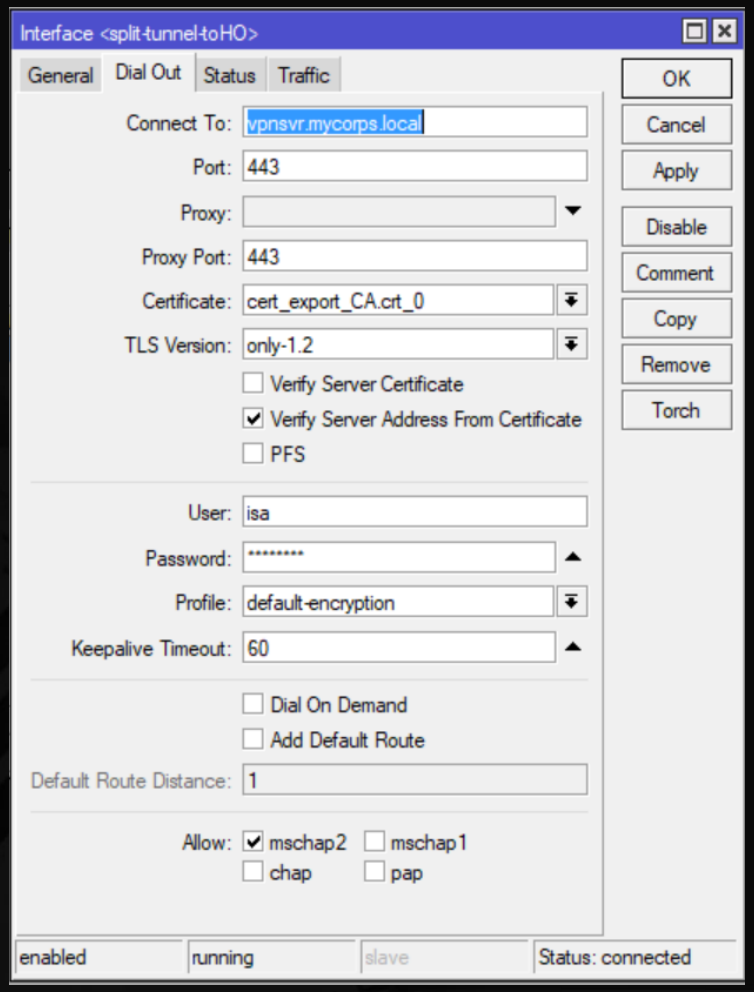


Enable SSTP Server Interface on Mikrotik HO

Mikrotik – Configure Mikrotik Branch as Split Tunneling VPN



Import Certificate Root CA + Private Key Mikrotik HO



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
```

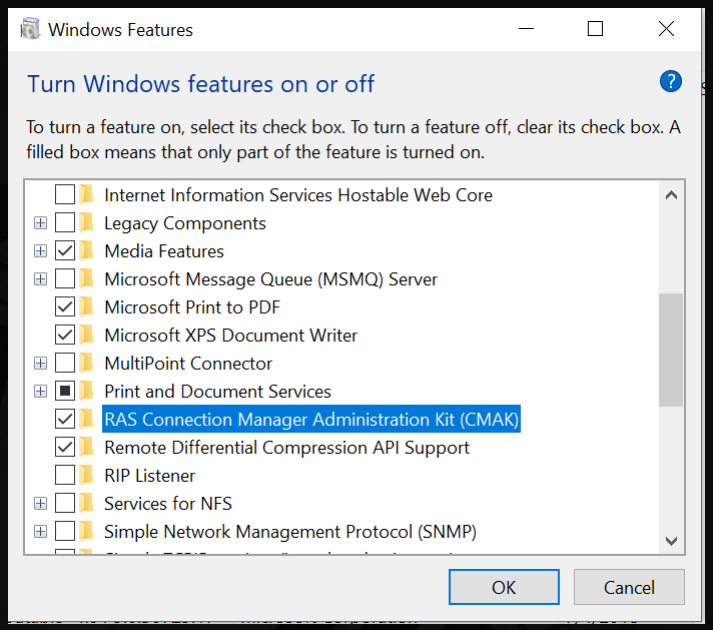
Result – Split the connection

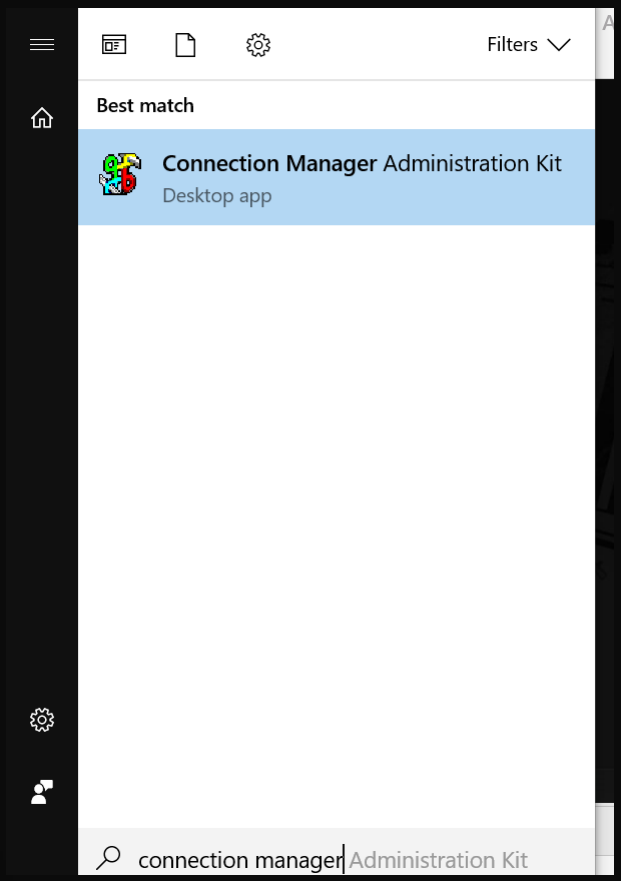
```
[admin@MikroTik] > tool traceroute 8.8.8.8
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 192.168.100.1                      0%    4   1.7ms     1.6     1.4     1.8     0.1
 2 10.89.0.1                          0%    4   4.4ms     4.3       4     4.6     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

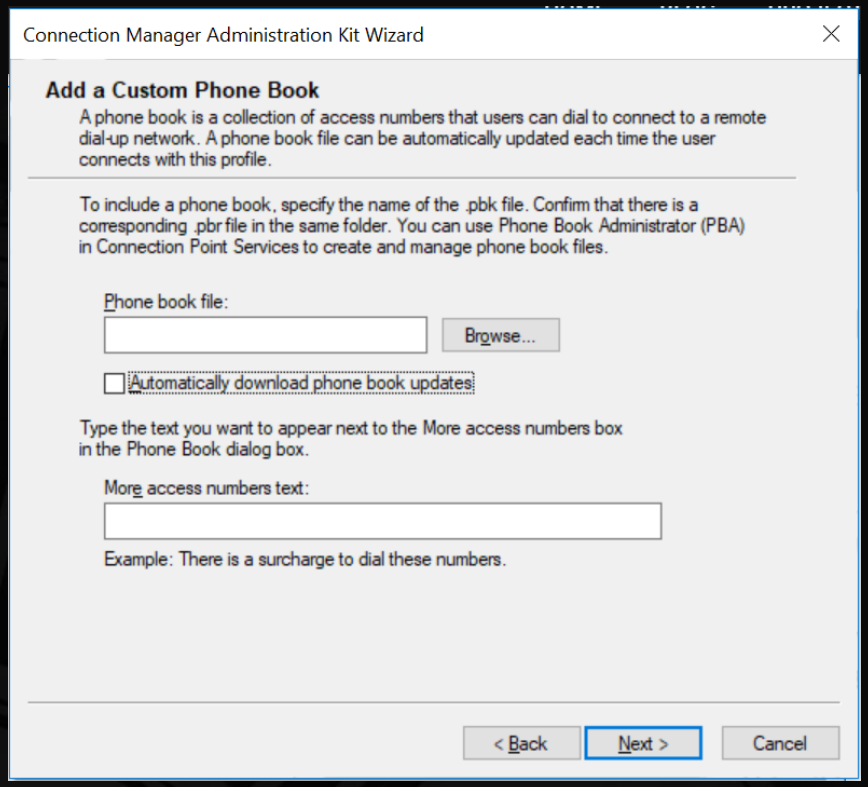
How do we split route on endpoints?

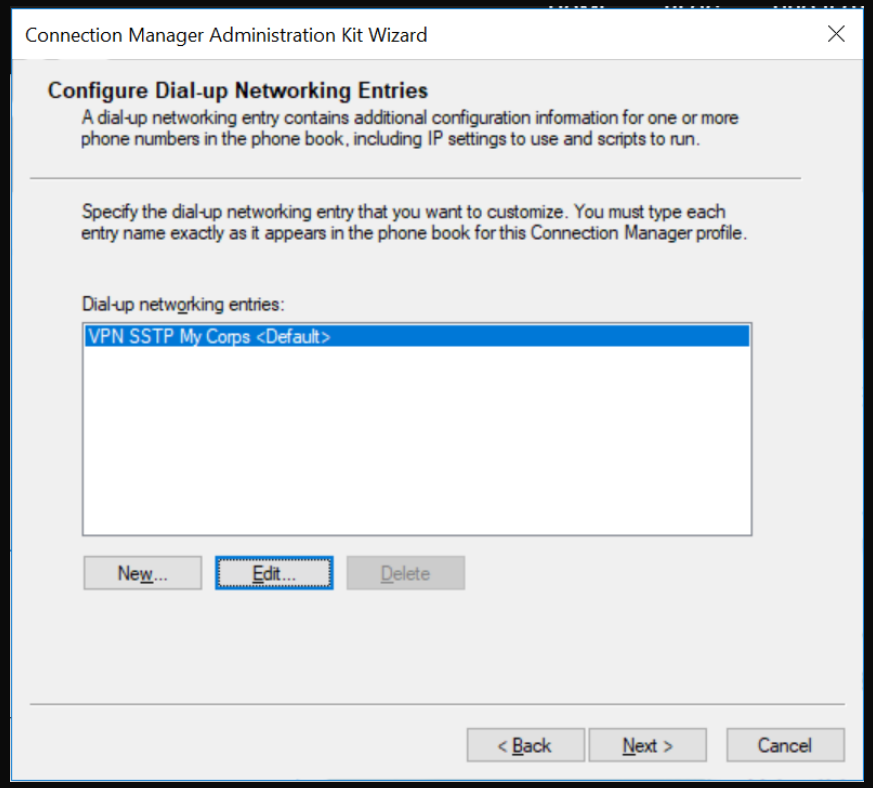
On >100 endpoints?





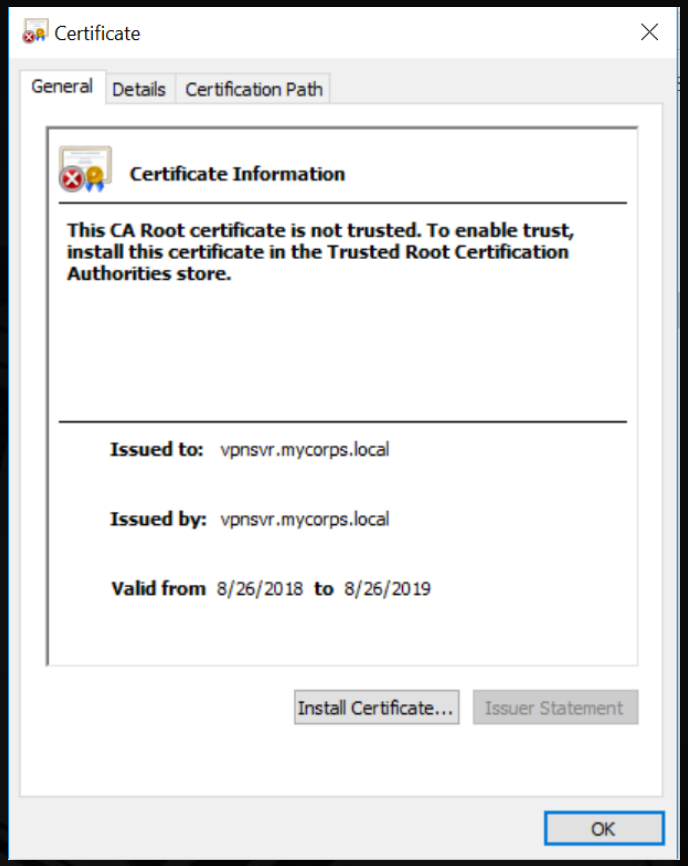
Create Executable Files VPN Profile with CMAK

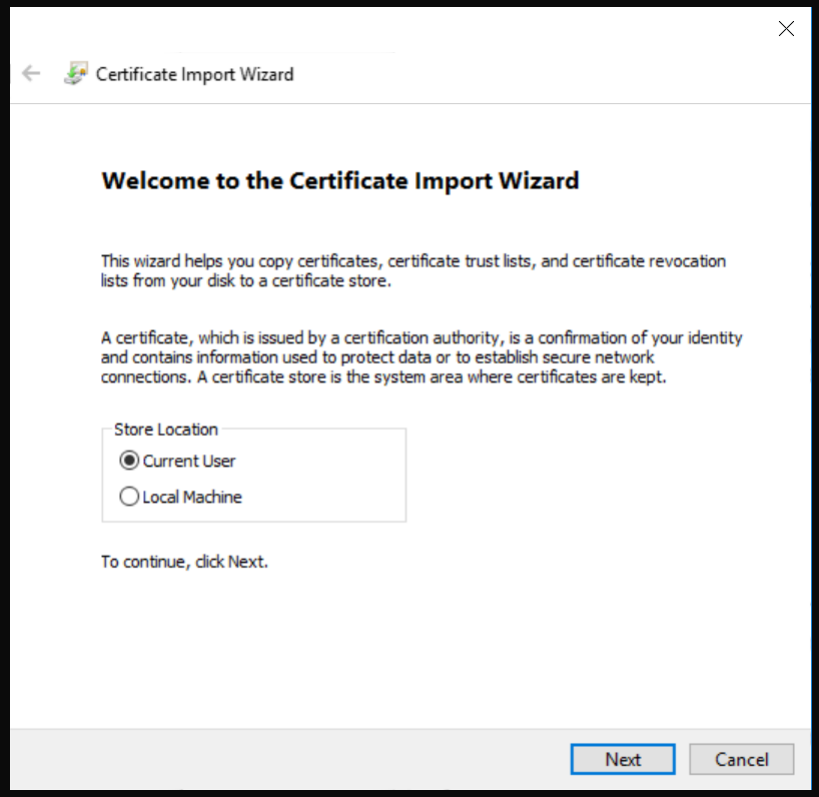




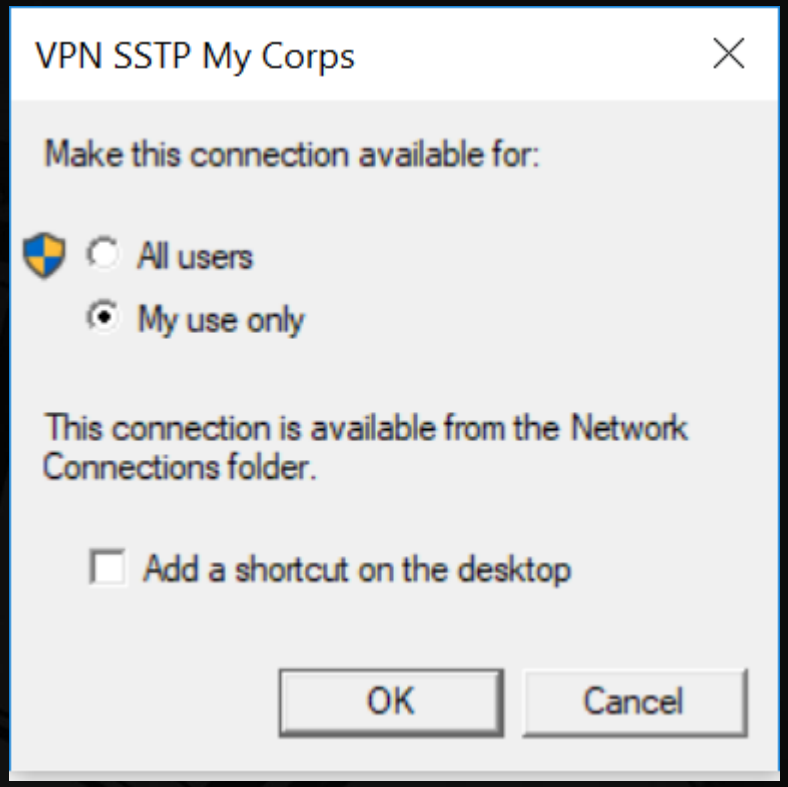
Create Route Table Profile for SSTP Client Interface

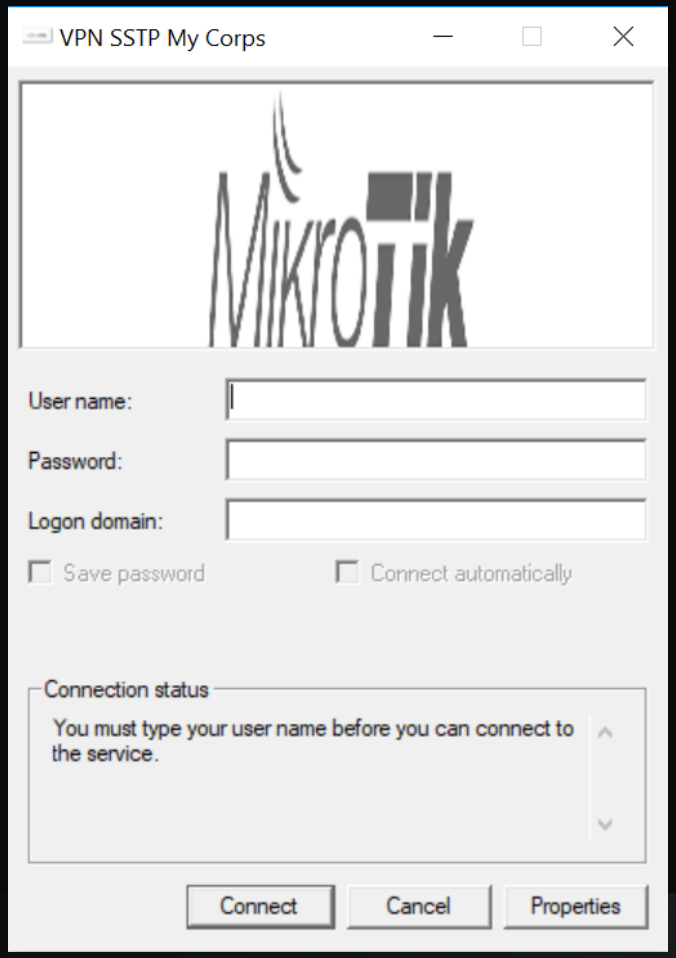
- Create a new txt file
- Define the routes will be through the VPN
- i.e -> ADD 192.168.100.0 MASK 255.255.255.0 default METRIC default **IF** default
- Save the file with .txt name
- Then, choose the file on CMAK





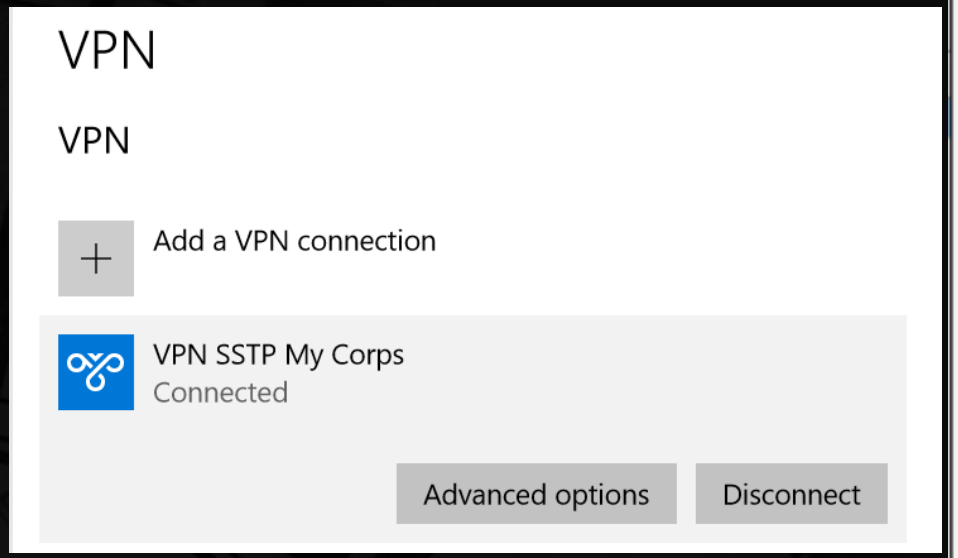
Import Certificate Root CA Mikrotik HO

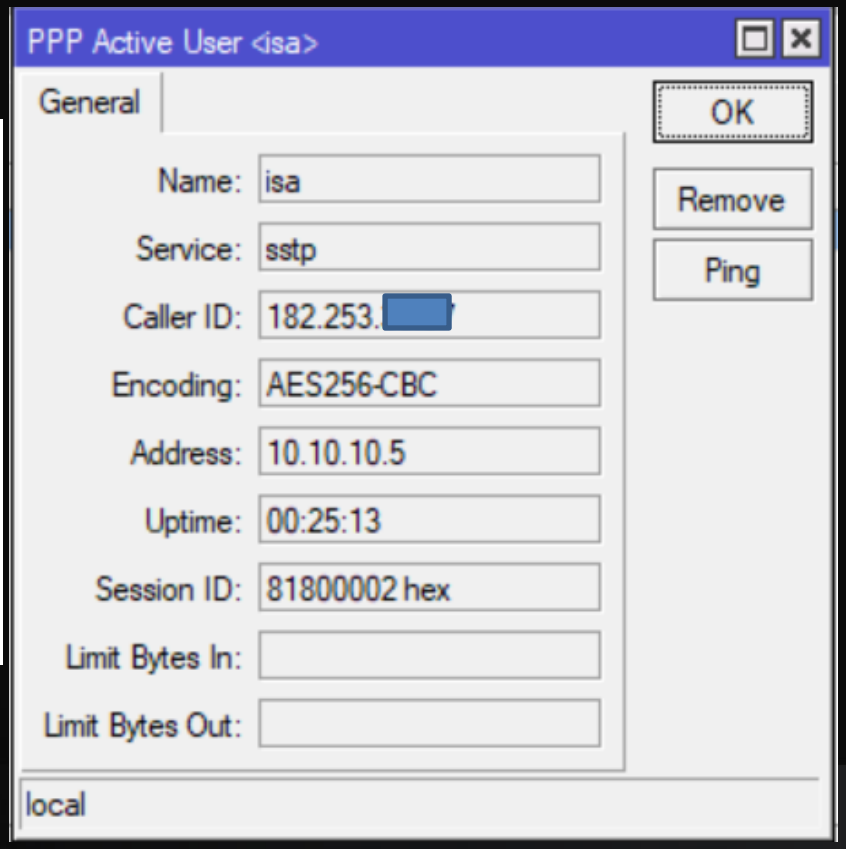




Install the executable file VPN SSTP Profile

Result – Without Split Tunnel



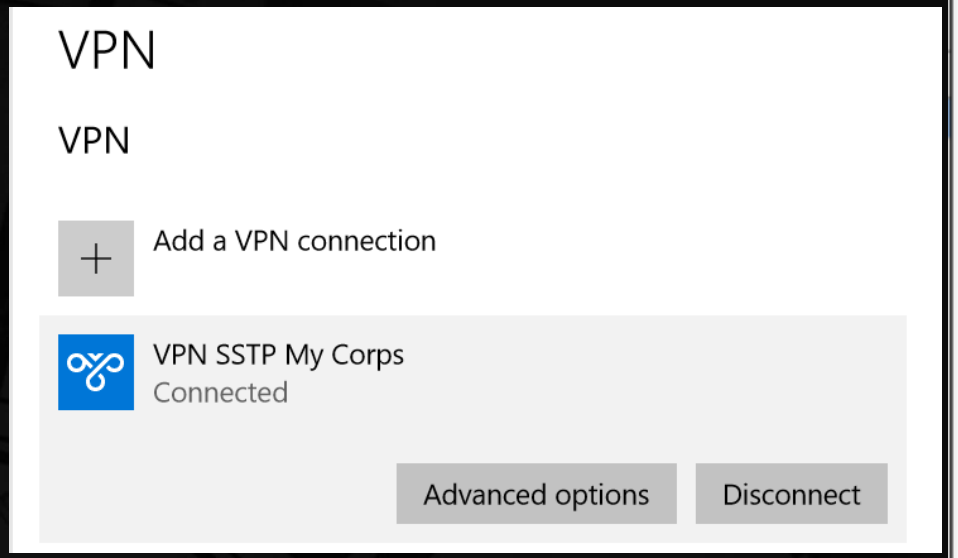


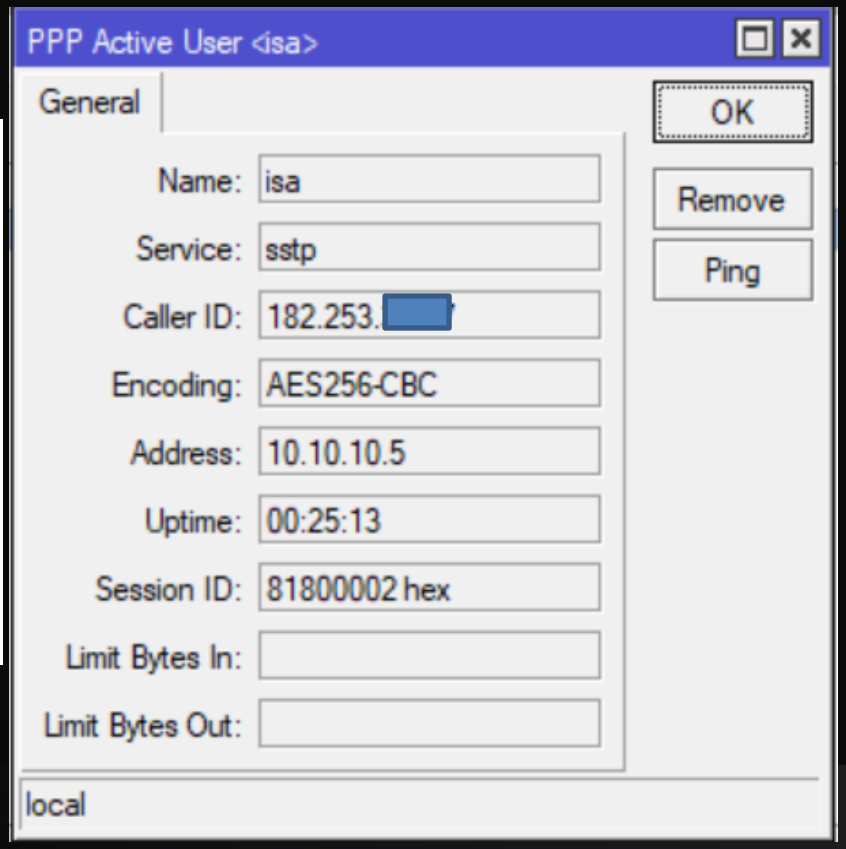
```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0         10.10.4.1      10.10.4.15   4260
          0.0.0.0          0.0.0.0         On-link        10.10.10.4     36
         10.10.4.0    255.255.255.0         On-link        10.10.4.15   4516
       10.10.4.15  255.255.255.255         On-link        10.10.4.15   4516
      10.10.4.255  255.255.255.255         On-link        10.10.4.15   4516
       10.10.10.4  255.255.255.255         On-link        10.10.10.4    291
     1[redacted].103.6[redacted].2  255.255.255.255        10.10.4.1      10.10.4.15   4261
        127.0.0.0        255.0.0.0         On-link         127.0.0.1   4556
        127.0.0.1  255.255.255.255         On-link         127.0.0.1   4556
  127.255.255.255  255.255.255.255         On-link         127.0.0.1   4556
     192.168.56.0    255.255.255.0         On-link      192.168.56.1   4506
     192.168.56.1  255.255.255.255         On-link      192.168.56.1   4506
   192.168.56.255  255.255.255.255         On-link      192.168.56.1   4506
    192.168.137.0    255.255.255.0         On-link     192.168.137.1   4536
    192.168.137.1  255.255.255.255         On-link     192.168.137.1   4536
  192.168.137.255  255.255.255.255         On-link     192.168.137.1   4536
    192.168.220.0    255.255.255.0         On-link     192.168.220.1   4516
    192.168.220.1  255.255.255.255         On-link     192.168.220.1   4516
  192.168.220.255  255.255.255.255         On-link     192.168.220.1   4516
    192.168.225.0    255.255.255.0         On-link     192.168.225.1   4516
    192.168.225.1  255.255.255.255         On-link     192.168.225.1   4516
  192.168.225.255  255.255.255.255         On-link     192.168.225.1   4516
        224.0.0.0        240.0.0.0         On-link         127.0.0.1   4556
        224.0.0.0        240.0.0.0         On-link      192.168.56.1   4506
        224.0.0.0        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	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
1[redacted].103.[redacted].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/yoisapangestu/

Isa.pangestu@outlook.com